Smart Borders Pilot
Interim Report on the technical conclusions of the Pilot project

supported by pwc

July 2015

Table of Contents

Executive Summary

Background

The COM-led Technical Study[1] (the first step of the Proof of Concept) identified the suitable options and solutions for the Smart Borders package to be tested during the Pilot. The aim of the Pilot (the second step of Proof of Concept) carried out by eu-LISA is to verify the feasibility of the proposed options and validate the selected concepts for both automated and manual border controls in operational environments with real travellers across Europe by November 2015.

Objective of Interim Report

The objective of the given report is twofold:

- Present the status and results of the Pilot as of 15 July[2] as an eu-LISA's contractual obligation towards COM[3];
- Give the first insight into the Final report and its possible structure.

To this end, this document provides **strictly preliminary** testing outcomes and does not reflect any final results or conclusions (see also Limitations section as the last paragraph of this chapter).

Status of Pilot

During the Pilot 78 tests are carried out across 18 border crossing points in 12 Member States.

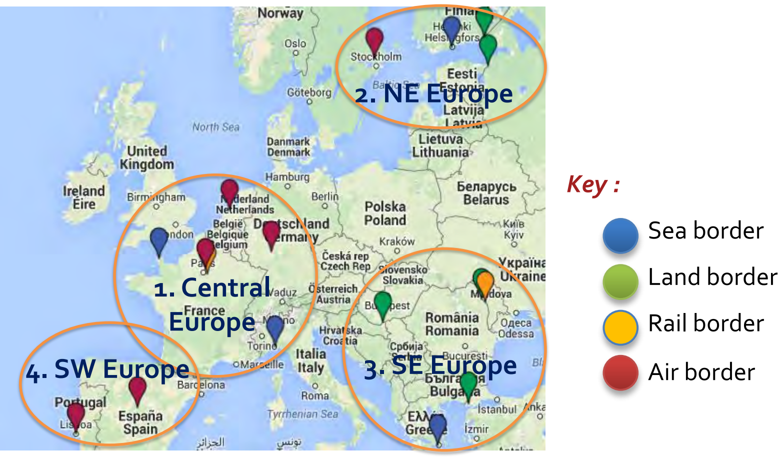


***Figure 1** Participating Member States and BCPs*

[1] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/smart_borders_report_/smart_borders_report_en.pdf
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_Study_en.pdf

[2] The results presented are based on data collected from Test Cases **until 25 June 2015**

[3] By 15 July 2015, eu-LISA shall submit to the Commission a mid-term report on the preliminary technical conclusions of the Pilot project. The detailed content of this report is described in the ToR included as an Appendix to Annex I (Delegation Agreement Article 19 – Report on the technical conclusions of the Pilot project)

The figure in the next page gives an overview of the total number of different operational tests included in each test case and their current status. It also outlines the ongoing tests (*i.e.* 51/78, 65%) as well as to the test finished in BCPs as of 25 June and included in the given report (*i.e.* 13/78, 17%).

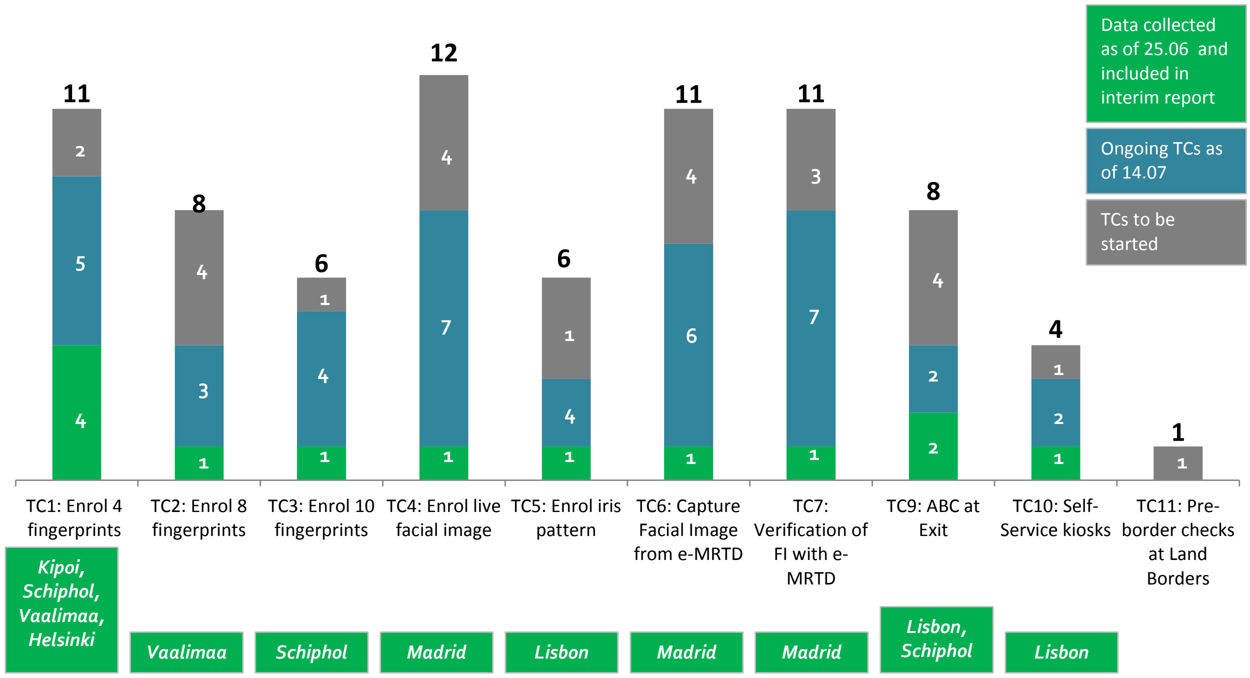


Figure 2 *Results analysed and included in Interim report as of 25.06.2015 compared to ongoing and total number of Test Cases*

In addition to operational test data, this report includes the preliminary results from desk research topics such as: VIS border using travel document number, fall-back measures, chip reading and iris spoofing.

Main observations

So far the execution of Test Cases has been smooth and Member States have been deeply engaged and committed, both in terms of border crossing points and border guards but also in terms of commitment in contributing actively towards the Pilot. Positive feedback regarding the use of the biometric identifiers and the related technology has been gathered not only from the border guards but also the travellers regard the test cases performed as a positive and more secure experience; especially at the air and sea borders.[4]

[4] This feedback could however be a consequence of standalone tests (*i.e.* a separate process on top of the normal border control process). This will be different in a future process where solutions are integrated in a border control process adapted to the novelties.

Travellers' feedback

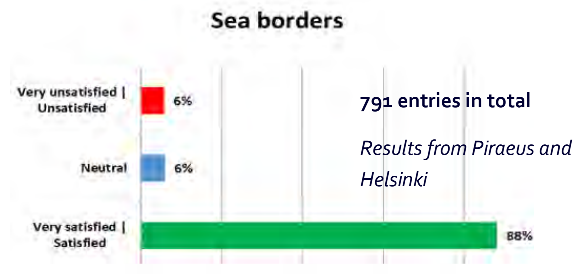


Figure 3 *Travellers' survey results as of 25.06.2015 at sea borders*

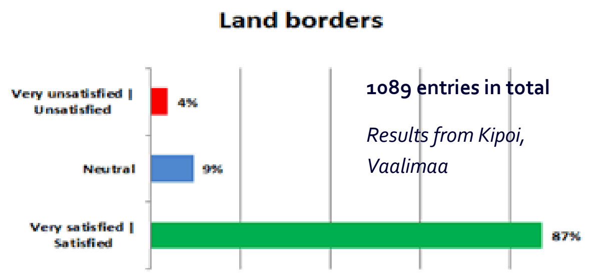


Figure 4 *Travellers' survey results as of 25.06.2015 at land borders*

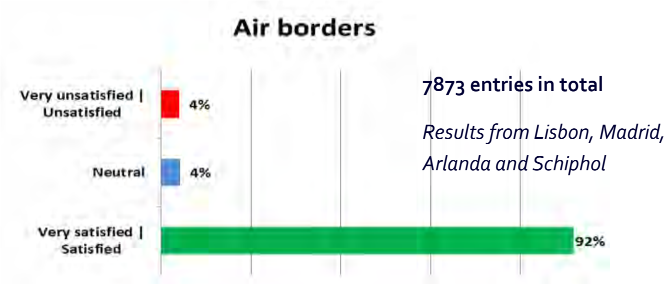
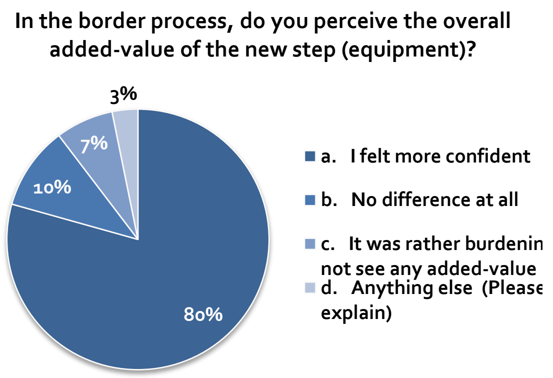


Figure 5 *Travellers' survey results as of 25.06.2015 at air borders*

Border guards' feedback[5]



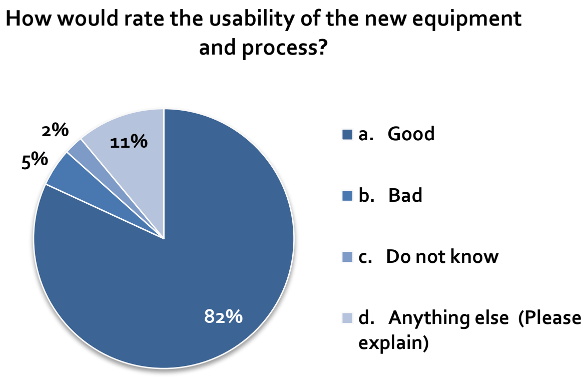


Figure 6 *Results of border guards' survey feedback as of 25.06.2015*

Figure 7 *Results of border guards' survey feedback as of 25.06.2015*

[5] Consolidated feedback based on data received from Madrid TC 1, 4, 6, 7 | Vaalimaa TC 1,2 | Lisbon TC5 | Kipoi TC1

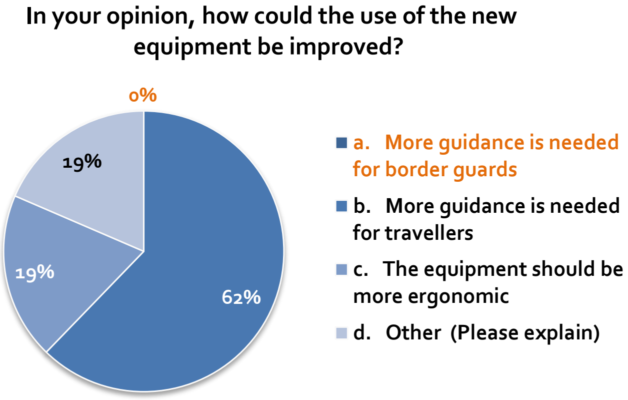


Figure 8 *Results of border guards' survey feedback as of 25.06.2015*

In addition, operational results are overall encouraging. Although some improvements are needed regarding specific details, the data provided give very interesting indications as regards usefulness, usability and impact in terms of the time required for including biometric identifiers at operational border crossing operations.

Attention points

Data included in this report must be interpreted with reservations. The following shall be taken into consideration:

- The results provided are only a fraction of the expected results (see Figure 1). They do not cover all the different options on use of biometric identifiers nor encompass data from all the type of borders or different technology tested;

- Most of the test data have been received very close to the due date of Interim report, hence, all data cleaning and quality checks could not be made;

- No comparison or assessment of the equipment used in testing will be given;

- Participating vendors will not be referred to;

- No judgement can be made about participating Member States, their national authorities or set-up of infrastructures of border crossing points;

- Gathered results are entirely dependent on the Member States border control processes and the way the individual tests have been set up and performed. Therefore, the report only shows objective information which shall be extrapolated carefully. For Final Report, the individual results (of different BCPs, TCs and equipment) will be furthered assessed and carefully processed with an attempt to bring them to an overall high-level comparability as much as possible;

- Complementary information to the test results, driven from further consultations and quality assurance with the relevant stakeholders (e.g. Member States experts, Frontex, industry), will be included at a later stage;

- The conclusions of the tests will only be reflected in the Final report.

Confidentiality

- This report is strictly for internal distribution and any external circulation must be avoided. External parties could be misled and make wrongful conclusions that could potentially hinder the further work on the Pilot and its results.

1. Introduction

Background

During the first examination of the Smart Borders Package (February 2014), the Council and the European Parliament (EP) voiced technical, operational and cost concerns related to the overall feasibility and some features of the Registered Traveller Programme (RTP) and the Entry / Exit System (EES). The concerns included the choice of biometric identifiers, the impact on the border crossing process and the extent to which national EES could be integrated and/or reused.

In order to further assess the technical, organisational and financial impact of the various possible ways to address these issues, the European Commission (COM) subsequently initiated – under mandate of COREPER and with the support of both co-legislators – a **Proof of Concept** exercise to identify options for the Smart Borders package implementation. This exercise is conducted in two stages:

- A COM-led **Technical Study**[6] (the Study) that identified and assessed the most suitable and promising options and solutions;

- A **Pilot** (or Testing Phase) which would verify the feasibility of the options identified in the Technical Study and validate the selected concepts for both automated and manual border controls. The Testing Phase has been delegated by COM to eu-LISA and it is to be run until November 2015.

Interim Report

The objectives of the Pilot are based on the **Terms of Reference** (ToR) issued by COM, as well as comprehensive instructions provided in the **Roadmap designed by eu-LISA**, which determine which options should be tested and which conditions could be met.

The purpose of this Interim Report is to provide an overview of the preliminary results of the ongoing Testing Phase of the Proof of Concept (also referred to as "the Pilot" or "the Project") for its main stakeholders, *i.e.* COM, EP and Member State representatives. The Interim Report serves as a draft for the Final Report (November, 2015) that will provide the Pilot's final results and conclusions.

This Interim Report is structured as follows:

- **Chapter 1** provides an introduction and background information about the Pilot, including the reasoning and its main objectives;
- **Chapter 2** describes the main methodologies employed and explains the overall approach for technical as well as data protection and analysis aspects;
- **Chapters 3 – 9** give preliminary answers to the questions raised in the ToR. The chapters are structured according to the various biometric modalities (fingerprints, facial image and iris) complemented by the accelerators. The answers are provided on the basis of the operational findings and desk research with regard to the ABC gates and kiosks. This information is further enriched by the findings from the pure desk research (VIS, fall-back scenarios and iris spoofing).

[6] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/smart_borders_report_/smart_borders_report_en.pdf
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_Study_en.pdf

2. Methodology

This chapter briefly describes the methodologies used and the approach followed during Pilot execution, including technical as well as data protection and analysis aspects. Overall set-up describes three main methodologies applied and selection of border crossing points (BCPs), while the approach for technical aspects covers the capturing of biometric quality indicators, timing information as well as the equipment and algorithms used.

2.1 Overall set-up

The Pilot employs three types of methodologies, each achieving different purposes, namely **operational testing integrated in border control processes, partial operational testing** and **desk research**.

Full operational testing is applied when the testing of the option is feasible in an operational environment or when MS provides the necessary resources to perform the adequate adaptations and measurements (human resources, infrastructure, required time, border guards and operators).

Full operational testing enables baseline measurement, where applicable, adaptation of the existing border crossing process to integrate an EES/RTP option and measurement of change indicators from the new process. It also makes it possible to calculate the difference between the existing process and the new process.

Partial operational testing is applied for new equipment testing when integration of equipment / systems is not manageable or not practical (e.g. integration of kiosk in existing system).

Concretely, partial operational testing makes it possible to introduce the option to be tested with minimal changes to the existing border crossing process and it makes it possible to test the feasibility of the option in real-life conditions.

The 18 BCPs (air, land and sea borders) selected in 12 Member States were **representative of the variety of Schengen border conditions** (e.g. border type, ABC gate types, land border with cars). The **biometric devices** used for the operational and partial operational tests were **already available on the market**.

As specified in Roadmap, **desk research** is applied in the following particular cases for specific topics as specified by the ToR (i.e. anti-spoofing methods for iris enrolment, fall-back options, VIS border check using travel document number) or when it is impractical or non-feasible (e.g. timeline, budget) to perform real-life testing.

Desk research includes literature review, outcome of interviews and workshops with stakeholders (e.g. FRONTEX, ABC Working Group, FRA, MS and industry), experiences from previous/similar projects (e.g. ABC4EU, FastPass, Tabula Rasa) and MS experts' group consultations.

2.2 Users' feedback

To analyse users' acceptance from workflow and perception aspects, feedback was collected both from travellers and border guards.

To draw **lessons learnt** from users in the field, participating border guards have been asked to provide feedback by filling in a questionnaire. This survey is made of five questions related to **value-added of new equipment** (1), its **usability** (2), **possible improvement of usability** (3), **acceptance of travellers** (4) and finally major **issues encountered** (5). Issues can be either travellers related or equipment related.

Additionally, the travellers have been asked to express their opinion about the testing process. The capture of the travellers' feedback has been done either by using a tablet after the test or a survey integrated in the mobile device. The traveller has the possibility to choose five smiley faces: ranging from very unsatisfied to very satisfied. Survey data are to be stored until the end of testing to enable the traceability, however data has been extracted, reviewed and analysed regularly.

2.3 Technical questions

2.3.1 Biometric quality measurement

With regard to **biometric quality measurement of fingerprints**, NFIQ and vendor specific quality scores are used, as requested by the ToR.

The Pilot refers to NIST NISTIR 7151 – also known as NFIQ v1 – under which fingerprint samples are ranked on a scale from 1 (excellent) to 5 (poor). Following consultations with the vendors on quality thresholds for fingerprinting, the emphasis is maintained that fingerprints should be enrolled to a sufficient quality to permit accurate 1:n identification in a database of 70 million people (in line with the current size of the VIS). Therefore, NFIQ is applied following these biometric thresholds:

- The little finger is enrolled with an NFIQ score of 3 or better;
- Other four main fingers of the hand are enrolled with NFIQ scores of 2 or better.

Vendor fingerprint quality indicators are proprietary and, as such, cannot be compared across vendors directly. However, they serve the purpose of estimating vendor-specific system performance.

Regarding the **quality assessment of facial images**, ICAO 9303 is used to evaluate the quality of the Facial Image stored in the e-MRTD. For live facial images, the use of vendor-specific algorithms results in higher granularity and greater relevance of the quality score in operational environments.

The ToR requests the use of prevailing quality indicators and vendor quality indicators for **quality assessment of the iris pattern.** Following consultation with vendors in the domain of iris pattern enrolment and verification, it has been decided that a set of characteristics from ISO/IEC 29794-6 must be used to assess the quality of enrolled iris patterns (e.g. uniformity, sharpness, roundness and dilation ratio).

2.3.2 Time measurement

The duration of the border control processes and of their respective individual steps is measured according to the following methodologies (or a combination thereof), depending on the Test Case and on the specific set-up at the different BCPs:

- **Time-stamped log files:** the software operating the different devices (e.g. FP scanners) records the events in a log file with a time stamp (synchronised via NTP, Network Time Protocol);
- **Clock On The Wall** (COTW): a timekeeper (border guard or assisting personnel) manually measures the time, using a stopwatch or specific desktop application.

2.3.3 Sampling

The overall principle for the choice of sample size was finding the right balance between the available resources for the test, passenger throughput per BCP and the desired confidence to make conclusions about the population from the sample.

During the execution of the Testing Phase, the amount of passengers per each Test Case at each BCP was monitored and compared against the target minimum sample size. This allowed the testing team to make any necessary adjustments during the execution (*i.e.* add extra staff, improve information/incentive activities, make some necessary adjustments to set-up or prolong the testing phase, if feasible).

2.4 Data collection and protection

Adequate **data protection measures** have been put in place. The data collected for the test has been depersonalised and saved only locally (*i.e.* kept separately from any other information that would make it possible to match the data with a person's identity) and the retention of that data has been limited to the time necessary to produce the relevant statistics and analysis.

In order to have personal data processed, the travellers have been informed of the type of data collected, the purpose of the processing and the controller's identity. The traveller has been explicitly and freely given his/her consent to participate in the test and has been also informed of his/her right as a data subject in accordance with data protection law.

The **data collection** and analysis process, as presented in the figure below, is based on the six following steps:

1. Collecting raw data from BCPs and mapping it to the Pilot's specifications;

2. Mapping the data;

3. Cleaning the mapped data based on 'technical' and 'business' rules, including format/ unit checks, consistency checks, date & time checks etc.;

4. Merging all cleaned data into a single data file;

5. Analysing the cleaned data with statistical methods;

6. Visualising the cleaned data and statistical analysis for business reporting purposes.

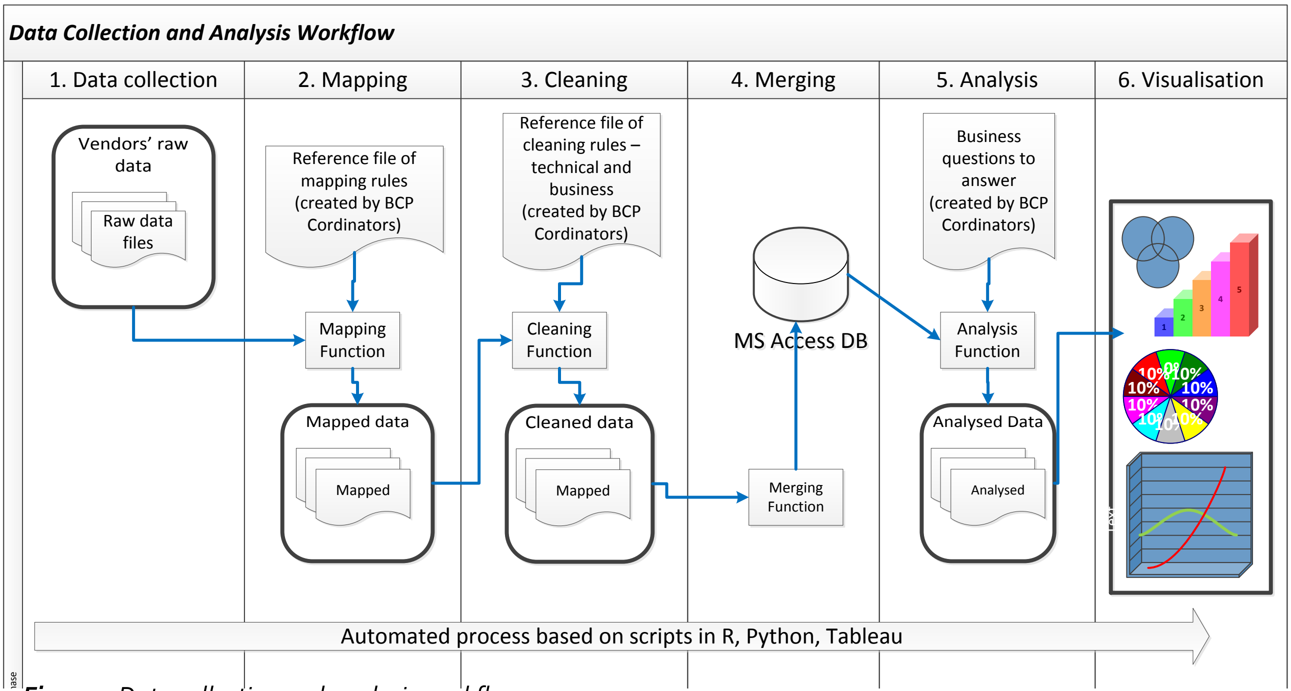

Data Collection and Analysis Workflow
1. Data collection
2. Mapping
3. Cleaning
4. Merging
5. Analysis
6. Visualisation
Vendors' raw data
Raw data files
Reference file of mapping rules (created by BCP Cordinators)
Mapping Function
Mapped data
Mapped
Reference file of cleaning rules – technical and business (created by BCP Cordinators)
Cleaning Function
Cleaned data
Mapped
MS Access DB
Merging Function
Business questions to answer (created by BCP Cordinators)
Analysis Function
Analysed Data
Analysed
Automated process based on scripts in R, Python, Tableau

Figure 9 *Data collection and analysis workflow*

1. Collecting raw data from BCPs. The original data were stored in unchanged conditions to enable the traceability of modifications introduced at further steps of data processing. Basic controls were performed to ensure that data do not contain any personal data or information out of the scope of the Pilot.

2. Mapping the original data to the Pilot's specifications. The mapping is done automatically and is based on the original mapping provided by the vendors or MSs. There were several issues with the files coming from vendors without any headers and column content specifications. This resulted in additional requests sent to the vendors, because the reference table containing all the possible vendor mappings is needed as an input for the automatic mapping procedure. The reference table was created by both the BCP coordinators and the data analysis team.

3. Cleaning the mapped data. The cleaning was performed automatically and is based on 'technical' and 'business' rules. The technical cleaning rules are common across all TCs and all BCPs and are as follows:

   - Check for empty rows. There were few cases observed and removal of them did not significantly affect the data;
   - Check for inappropriate symbols (N/A, '-', N/A, etc.) and substitute them with a blank space. This allows for more appropriate recognition of numeric values by visualisation / analysis tools;
   - Check that only third country nationals were participating in the Pilot, as demanded by the Terms of Reference.

   The following business cleaning rules are developed by the BCP coordinators and might differ per TC or per BCP:

   - Check for data being within appropriate intervals as defined by BCP coordinators in agreement with the vendors and test teams. If falling outside the identified range, the content is removed not only from the current cell, but from all cells of the row belonging to the same modality (FP, IR or FI). This reduced the noise in the data introduced either by erroneous attempts or by device errors, or by interactions that are outside of the standard usage in testing;

- Check for duplicated attempts. For some of the test cases and locations, the duplicates represented the largest proportion of removed data allowing significant reduction of noise. Rules for detection of duplicates differ per TC and/or BCP.

The output of the cleaning process consists of two files:

- The original file coming from the vendor, with information detailing observed issues to enable traceability on the changes introduced during the cleaning process;
- Another file with the cleaned data, *i.e.* content of cells with inappropriate data or the complete rows are removed from the file according to the rules above.

Although the automation of the cleaning process allows fast cleaning of the complete set of available data, the checks sometimes reveal issues with original data provided. This in turn requires further communication to MSs, vendors and/or border guards involved in testing, as well as the update of the cleaning rules. One of the issues currently observed concerns the acceptable ranges for durations of the border control processes. For the moment, the upper margin is set to an empirical value, whereas the most reasonable approach would be adjusting this value based on the statistical characteristics of the dataset. This question is scheduled to be addressed in the final report. Besides, the data received shortly before the deadline for the interim report are not included into the report.

4. Merging all cleaned data into a single data file. The data merging is done automatically. The merging can optionally be made per BCP or per vendor to optimize the visualization or data analysis. The final file will serve as an input for the visualization procedure.
5. Analysing the cleaned data with statistical methods.
6. Visualising the cleaned data and statistical analysis for business reporting.

3. Fingerprints

[Treatment and cleaning of data to be finalised in the Final Report]

3.1 Introduction

Today, fingerprints (FPs) are the most commonly used biometric modality for visa verification. However, the devices used vary greatly with different features and set-ups, and these results in different performance levels and variations in the duration of border crossing processes.

The latter factors are also highly dependent on the number of fingerprints used. A higher number of fingerprints enrolled results in a better performance in terms of accuracy and processing time, when they need to be used at a later stage for verifications or identification. However, the enrolment of more FPs might be problematic, as it might lead to problems in certain situations such as border checks on trains or ships. Therefore, not only different technical solutions have been taken into account during this Pilot, but also different amounts of fingerprints – as was already suggested in the Technical Study.

3.1.1 Objective

The objective of fingerprints enrolment testing is to evaluate the feasibility, user acceptance, timing and the delivered quality of enrolling fingerprints from TCNVEs at each type of border crossing (air, sea, land) in various conditions. Fingerprints verification which would add value for performance benchmarking between biometric modalities is not performed. In such case enrolled fingerprints and the traveller's identity would have had to be stored in order to test the verification either at exit and/or at a later re-entry. This would have required setting up a database where personal data and biometrics are recorded and have much longer timeline for the Pilot so to have enough exits matched and/or seconding entries. Thus due to timeline and data protection constraints to test fingerprints verification, only performance prediction calculated by vendors is provided.

The following test cases have been carried out[7]:

- **TC1:** 4 fingerprints (index, middle, ring, little) of the right hand (unless not present);
- **TC2:** 8 fingerprints (index, middle, ring, little) of the left and the right hand;
- **TC3:** 10 fingerprints.

The Pilot's objective of assessing the applicability of different fingerprint scanning solutions at different types of borders has been addressed in this section following the structure below.

1. **Operational and technical questions**

   a. **Success/ failure rates**

- What is the percentage of successful enrolment cases for different fingers?

   b. **Quality**

[7] TC9 (Automated Exit Checks of TCNs) and TC10 (Use of Self-Service kiosks) can also include FPs testing, however the results of those TCs are analysed in chapters6 and 0 of the Report.

- The quality indicators retained should make it possible to give clear estimates (after extrapolation) as to the AFIS's performance (accuracy, FTE, FRR, FAR). The quality indicators should be based on industry standards.

  c. **Duration**

- What is the added duration for enrolling fingerprints compared to the current situation where no biometric identifier is enrolled and therefore also verified for TCNVEs? These values need to be recorded according to the type of border and environmental conditions that cannot be controlled (like the external temperature).

1. **Users' feedback**

   a. **Perceived benefits by border guards**

- How do border guards experience the changes made to the border control process?

  b. **Perceived benefits by TCNs**

- What is the traveller's perception of the border control process?

2. **Constraints**

   a. **Environmental conditions**

- Which environmental conditions influence the quality and/or duration of the enrolment (e.g. temperature in outside conditions) at the different types of borders?

3. **Feasibility**

- Can fingerprints be enrolled at all types of border (air, sea and land) with the same devices as those used for fingerprint verification of TCNVHs? If not, which other devices would need to be installed at the enrolment desk?
- In the case of land borders, can fingerprints be enrolled and verified when passengers remain in the car or is a different set-up required? Is this also possible for bus travellers?
- Can fingerprints be enrolled using mobile equipment on trains?
- Can fingerprints be enrolled using two fingerprints mobile scanners?

3.1.2 Workflow of fingerprints enrolment

As indicated in the ToR, the enrolment of fingerprints follows the same process as for the enrolment in the VIS *i.e.* to assure the usability of the fingerprints captured, a minimum quality threshold is defined. As a general rule, if the fingerprints taken do not meet the quality criteria, a further attempt is made, up to three times.

Depending on the specific BCP, the testing of this step has either been integrated to their existing workflow or has been performed as a stand-alone step. For more information about the different workflows of TC1, 2 and 3, please refer to appendix 5 (paragraph 10.3.1), which provides detailed process maps of tests execution at all BCPs.

3.2 Methodology

TC1 (4 fingerprints enrolled), TC2 (8 fingerprints enrolled) and TC3 (10 fingerprints enrolled) testing is carried out in controlled and supervised environments, *i.e.* either the hostess or the border guard is assisting the traveller. The capture process has taken place in various settings to ensure representativeness of different BCPs across the Schengen Area:

- airport setting;
- seaport setting;
- fixed land-border setting (cars, trucks, buses);
- 'moving' land-border setting (trains with border guards).

The settings include testing the use of different types of biometric devices: existing technology at border posts, latest-generation fingerprint scanners, handheld devices etc.

TC1, 2 and 3 execution is often combined with other TCs, such as TC4 (FI enrolment), TC6 (FI capturing from e-MRTD) or TC7 (verification of live FI against FI captured from e-MRTD). This is done in order to minimise the cost and complexity of setting up and monitoring the testing, but also to reach a higher sample size per each test case. However, TCs involving the enrolment of a different number of fingerprints, *i.e.* TC1, TC2 and TC3 are never executed sequentially, so that one traveller would only give prints for enrolment on one scanner and the results would not be affected by the learning effect.

3.2.1 BCP Selection

BCPs where TC1 is executed:

Air

- Frankfurt (DE)
- Schiphol (NL)
- Madrid (ES)

Sea

- Port of Piraeus (EL)
- Helsinki port (FI)
- Cherbourg (FR)
- Genoa (IT)

Land

- Kipoi (EL)
- Vaalimaa (FI)
- Udvar (HU)
- Iasi (RO)

BCPs where TC2 is executed:

Air

- Frankfurt (DE)
- Schiphol (NL)
- Charles de Gaulle (FR)

Sea

- Helsinki (FI)

Land

- Kipoi (EL)
- Vaalimaa (FI)
- Iasi (RO)

BCPs where TC3 is executed:

Air

- Frankfurt (DE)
- Schiphol (NL)

Sea

- Helsinki (FI)

Land

- Udvar (HU)
- Kipoi (EL)
- Vaalimaa (FI)

This interim report only gives an insight into the preliminary data gathered from Helsinki (TC1), Vaalimaa (TC1 and TC2), Kipoi (TC1), and Schiphol (TC1 and TC3).

3.2.2 Type of equipment

The tests were carried out with different types of equipment. A brief overview of each of them is provided in the table below, also indicating the BCPs where the equipment type was used.

Table 1 *Type of equipment per different BCP*

Type of equipment	Description	BCP
Mobile FP scanners	Can be freely transported and operated without space limitation and do not require a client PC.	Kipoi (EL), Piraeus (EL), Iasi (RO)
Existing fixed FP scanners	Existing FP scanners used for verification of TCNVHs that require a client PC.	Udvar (HU), Schiphol (NL), Frankfurt (DE), Madrid (ES), Genoa (IT)
New fixed FP scanners	The latest-generation FP scanners that require a client PC.	Vaalimaa (FI), Helsinki (FI), Charles de Gaulle (FR), Cherbourg (FR)
Contact scanners	Requires the traveller to place his fingers on the sensor.	Kipoi (EL), Piraeus (EL), Iasi (RO), Vaalimaa (FI), Helsinki (FI), Charles de Gaulle (FR), Cherbourg (FR), Udvar (HU), Schiphol (NL), Frankfurt (DE), Madrid (ES), Genoa (IT)
Contactless scanners	Doesn't require a contact between the fingers of the traveller and the sensor.	Frankfurt (DE), Charles de Gaulle (FR), Schiphol (NL)

3.2.3 Configuration per BCP

3.2.3.1 Helsinki (TC1)

Table 2 *TC1 Helsinki seaport – TC configuration*

Duration of the test	3.5 weeks
Timetable of the tests	From 15.04.2015 to 08.05.2015
Layout	1 lane at exit and 1 lane at entry
Sample size achieved	602 (327 at exit and 275 at entry[8])
Technical integration	Integrated
Integration within the regular border crossing process	Integrated
Equipment type	Fixed
Enrolment/verification threshold	NFIQ and vendor specific

[8] Only entry data is included in the Interim report analysis.

Travellers' survey	Survey on tablet
Test personnel	2 border guards per shift

3.2.3.2 Kipoi (TC1)

Table 3 *TC1 Kipoi land border – TC configuration*

Duration of the test	3 weeks
Timetable of the tests	From 20.04.2015 to 11.05.2015
Layout	No dedicated lane; testing executed in the area around the BCP
Sample size achieved	680 at entry
Technical integration	Stand-alone
Integration within the regular border crossing process	Not integrated
Equipment type	Mobile
Enrolment/verification threshold	NFIQ
Travellers' survey	Survey on tablet
Test personnel	2 border guards per shift

3.2.3.3 Vaalimaa (TC1 and TC2)

Table 4 *TC1 Vaalimaa land border – TC configuration*

Duration of the test	2 weeks
Timetable of the tests	From 13.04.2015 to 27.04.2015
Layout	1 lane at exit and 1 lane at entry
Sample size achieved	648 (481 at entry and 167 at exit[9])
Technical integration	Integrated
Integration within the regular border crossing process	Integrated
Equipment type	Fixed
Enrolment/verification threshold	NFIQ and vendor specific
Travellers' survey	Survey on tablet
Test personnel	2 border guards per shift

Test Case 2

Table 5 *TC2 Vaalimaa land border – TC configuration*

Duration of the test	5 weeks
Timetable of the tests	From 27.04.2015 to 06.06.2015
Layout	1 lane at exit and 1 lane at entry
Sample size achieved	760 (538 at entry and 222 at exit[10])
Technical integration	Integrated

[9] Only entry data is included in the Interim report analysis.
[10] Only entry data is included in the Interim report analysis.

Integration within the regular border crossing process	Integrated
Equipment type	Fixed
Enrolment/verification threshold	NFIQ and vendor specific
Travellers' survey	Survey on tablet
Test personnel	2 border guards per shift

3.2.3.4 Schiphol

Test Case 1

Table 6 *TC1 Schiphol airport – TC configuration*

Duration of the test	3 Weeks (from the 22.04.2015 to the 12.05.2015)
Timetable of the tests	Weekday mornings
Layout	Single manual booth
Sample size achieved	1662 at entry
Technical integration	Standalone
Integration within the regular border crossing process	Integrated
Equipment type	Fixed Contactless
Enrolment/Verification Threshold	NFIQ 3 – 3 – 3 – 4
Traveller's survey	Self-service tablets on stands, introduced by host
Test personnel	2 to 3 Border Guards (1 at the booth, 1 to 2 to route the travellers and assist when needed) + 2 Hostesses before the test + 1 host for traveller's feedback

Test Case 3

Table 7 *TC3 Schiphol airport – TC configuration*

Duration of the test	3 Weeks (from the 12.05.2015 to the 02.06.2015)
Timetable of the tests	Weekday mornings
Layout	Single manual booth
Sample size achieved	1420
Technical integration	Standalone
Integration within the regular border crossing process	Integrated
Equipment type	Fixed contact
Enrolment/Verification Threshold	NFIQ 2 – 2 – 2 – 3 – 4
Traveller's survey	Self-service tablets on stands, introduced by host
Test personnel	2 to 3 Border Guards (1 at the booth, 1 to 2 to route the travellers and assist when needed) + 2 Hostesses before the test + 1 host for traveller's feedback

3.2.4 Sample characteristics

This section of the Report provides the description of sample characteristics, looking into the full dataset per gender, nationality and age range.

3.2.4.1 Helsinki

Test Case 1

Even though there were 275 travellers enrolled for TC1 in Helsinki at entry, after the data cleaning the sample size amounted to 272 travellers.

As shown in the figures below, most of the 272 participants were Russian with the dominant share of 95%. The majority (44%) of the travellers were 31-50 years old and there was a higher share (58%) of female travellers.

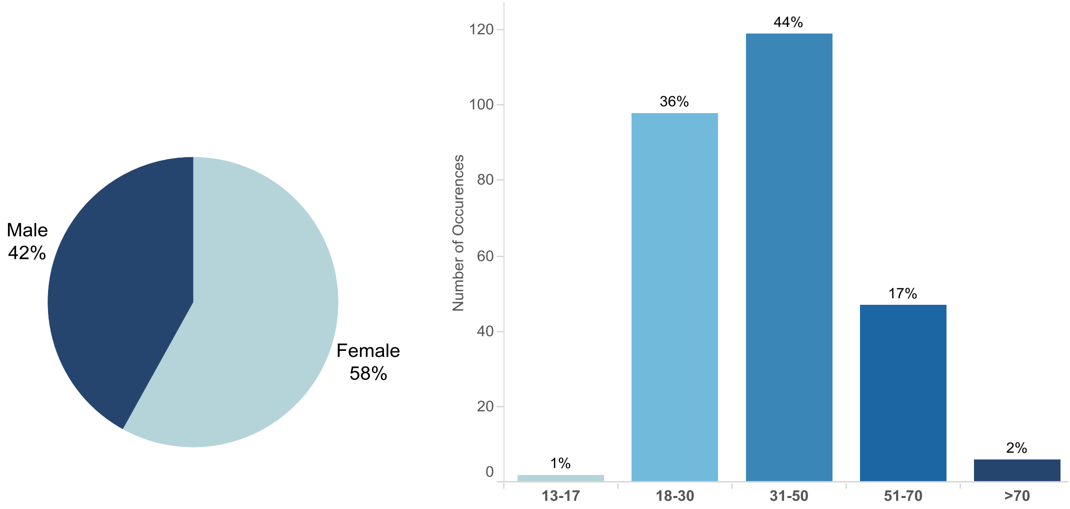


Figure 10 *TC1 Helsinki seaport - Sample characteristics per gender and age*

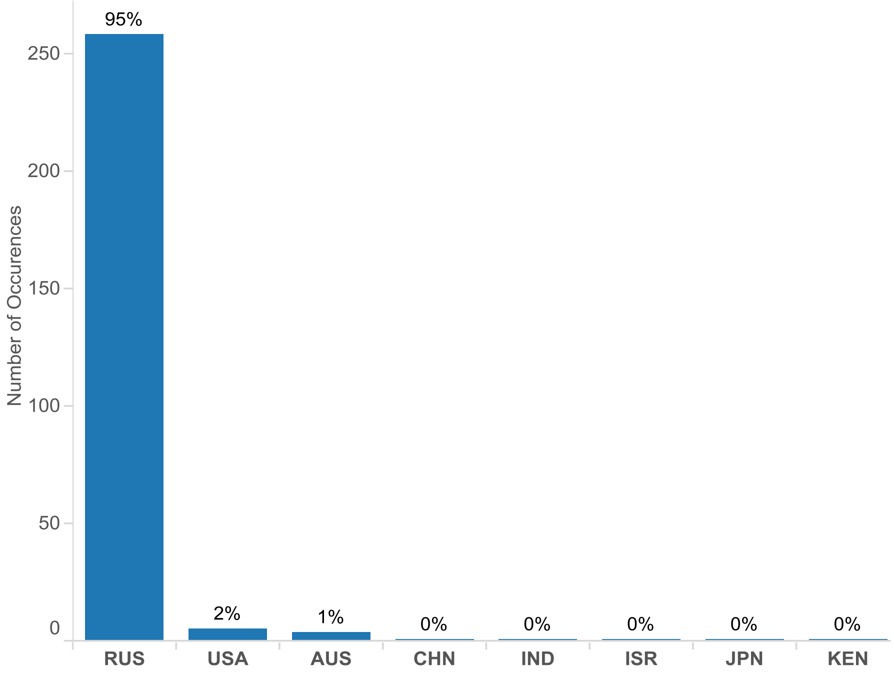


Figure 11 *TC1 Helsinki seaport - Sample characteristics per nationality*

3.2.4.2 Kipoi

Test Case 1

The initial sample size of 680 travellers in Kipoi was reduced to 639 after the data cleaning. The sample size could be characterised by a very low share of female travellers enrolled, which amounted to only 13%, as the travellers were mainly lorry drivers. Though there were travellers enrolled from all age groups, most of them (89%) were between 31 and 70 years old. Turkish was the main nationality of the travellers, with a 62% share.

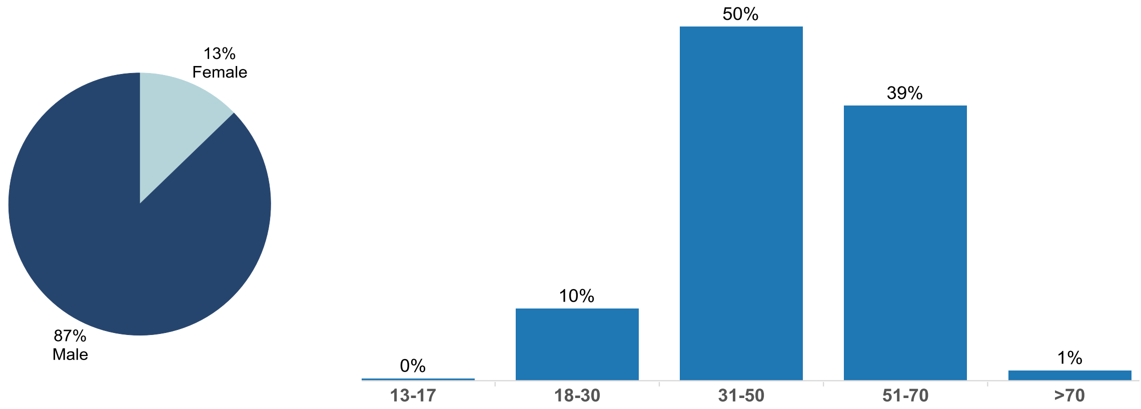


Figure 12 *TC1 Kipoi land border - Sample characteristics per gender and age*

3.2.4.3 Vaalimaa

Test Case 1

Male travellers comprised only a slightly higher share (54%) than female travellers in Vaalimaa. Since the Pilot was executed on the border with Russia, the participants were almost exclusively (99%) Russians. There were travellers enrolled from all age groups, however most of them (78%) were between 31 and 70 years old.

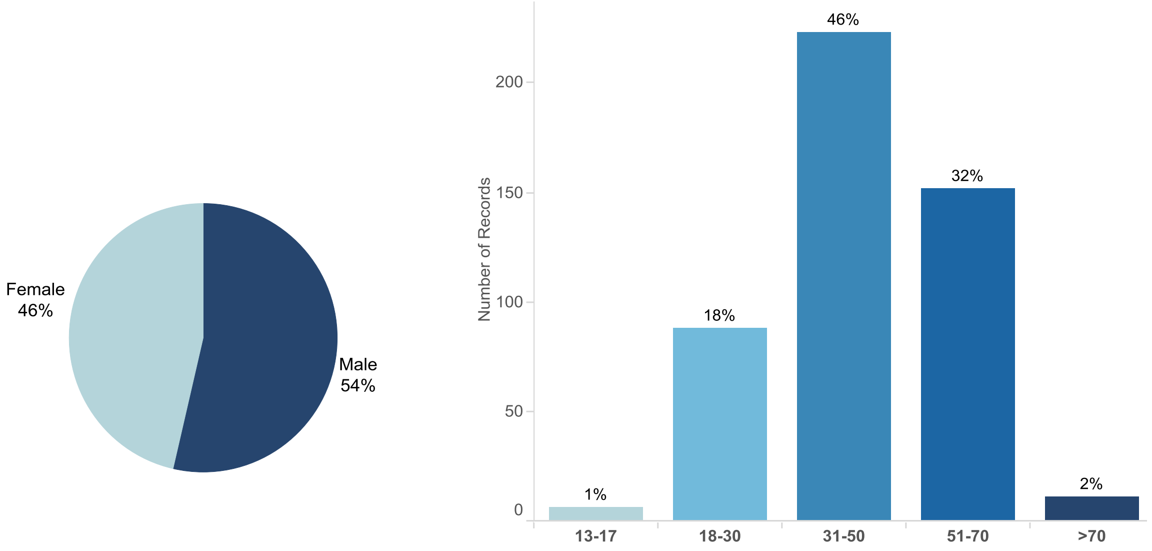


Figure 13 *TC1 Vaalimaa land border - Sample characteristics per gender and age*

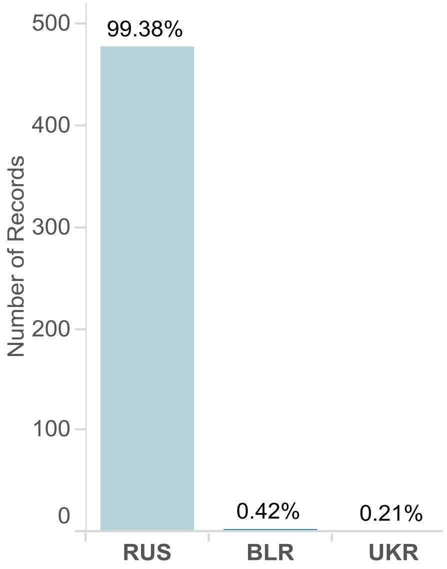


***Figure 14** TC1 Vaalimaa land border - Sample characteristics per nationality*

Test Case 2

After the data cleaning, the sample size for TC2 in Vaalimaa at entry amounted to 538 travellers. Similar numbers of male and female travellers were enrolled. Since the Pilot was executed on the border with Russia, the participants were almost exclusively (99%) Russian and they were mostly aged between 31 and 70 (82%).

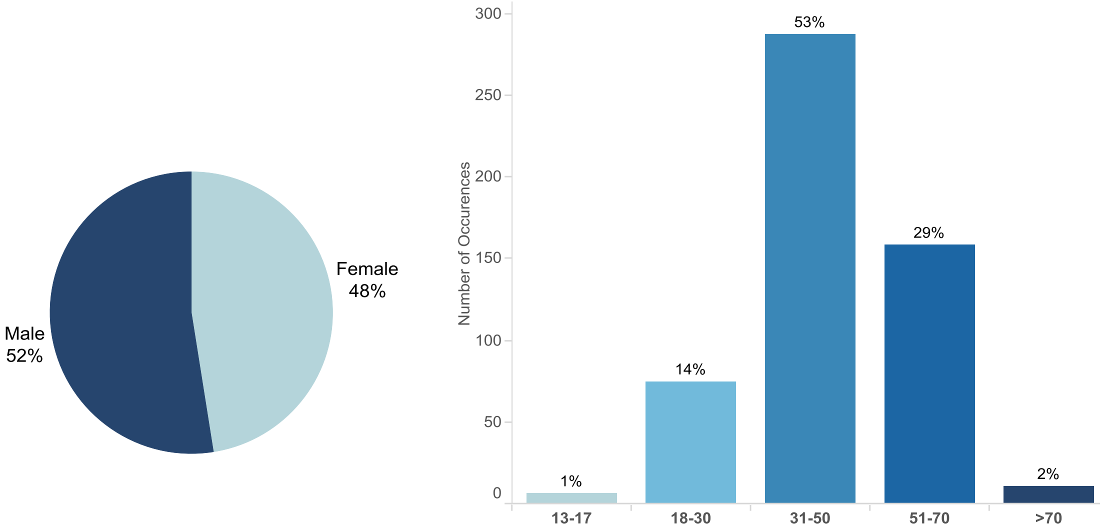


***Figure 15** TC2 Vaalimaa land border - Sample characteristics per gender and age*

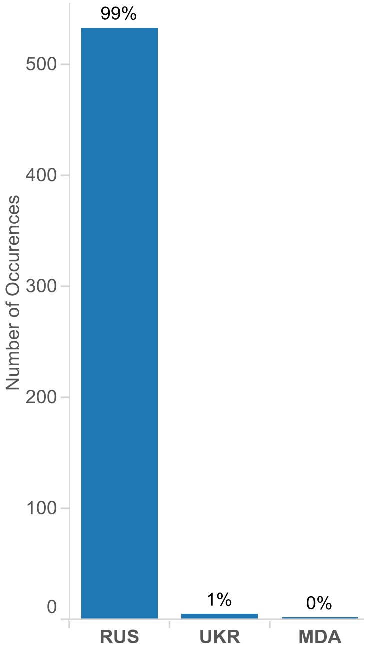


Figure 16 *TC2 Vaalimaa land border - Sample characteristics per nationality*

3.3 TC1 Technical and operational questions

3.3.1 Success/failure rate

The success condition is the successful capture of the fingerprint, above a given threshold and within three attempts. The threshold was based on NFIQ with the following values:

- For the little finger: NFIQ score of 3 or better;
- For the ring finger: NFIQ score of 2 of better.

3.3.1.1 Helsinki

The results of the successful attempts captured for each of the fingers with an optical scanner are provided in the figure below. The data show that the enrolment of the little finger was the most successful due to lower threshold applied, *i.e.* it succeeded in 88% of the cases in the first attempt, whereas the enrolment of the ring finger was the least successful.

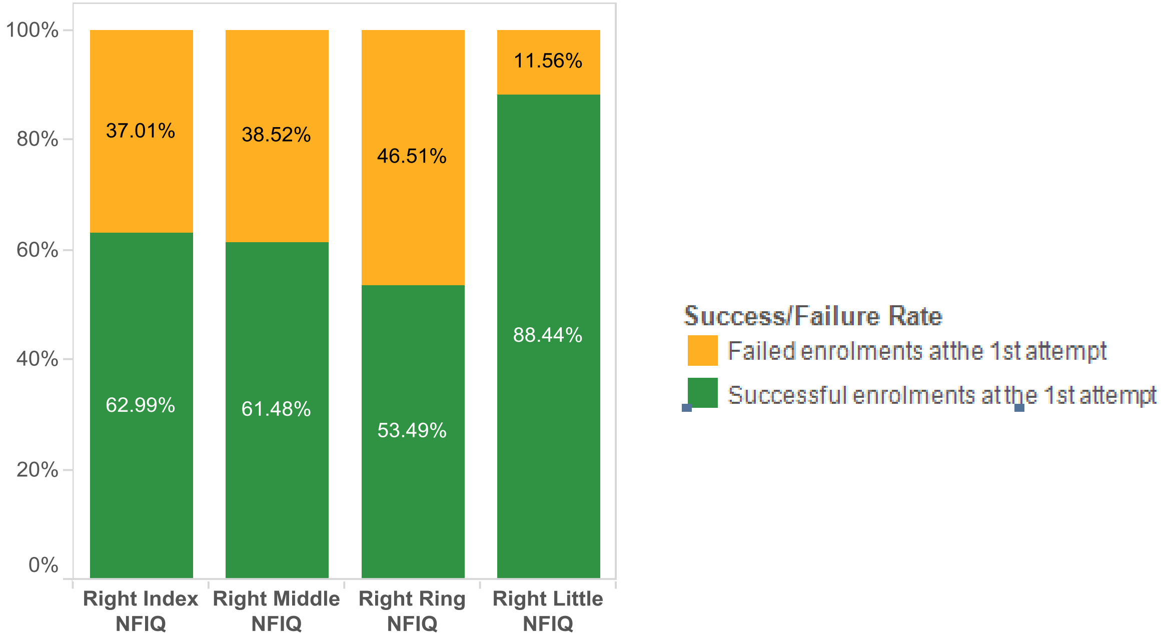


Figure 17 *TC1 Helsinki seaport - Results of successful and failed enrolments at the first attempt*

3.3.1.2 Kipoi

The number of successful enrolments at the first attempt in Kipoi represents a very large share. It varies from 84% for the little finger to 62%. This could be attributed to the fact that a Light Emitting Sensor (LES) scanner, not an optical one, was used, thus it was more conducive to outdoor conditions and also to the fact that the use of a two-finger scanner is easier than four together for passengers, albeit much slower.

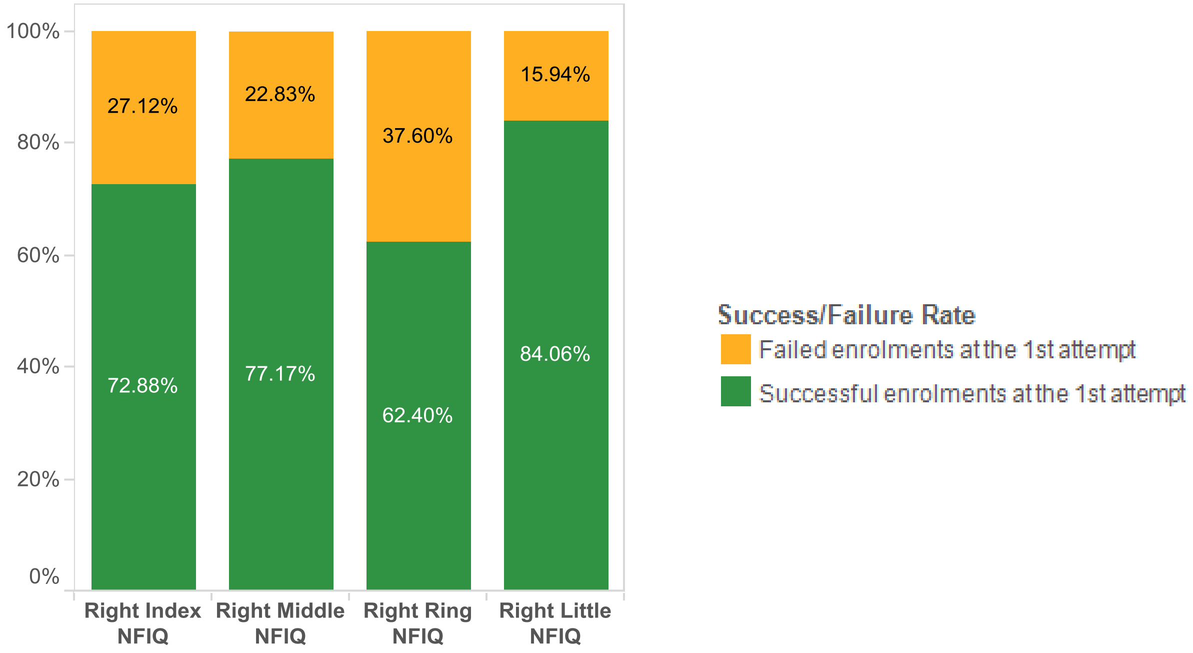


Figure 18 *TC1 Kipoi land border - Results of successful and failed enrolments at the first attempt*

3.3.1.3 Vaalimaa

The results of the successful attempts for each of the fingers are provided in the figure below. The data show that the enrolment of the little finger was the most successful, *i.e.* it succeeded in 81% of the cases in the first attempt, whereas the enrolment of the index finger was the least successful.

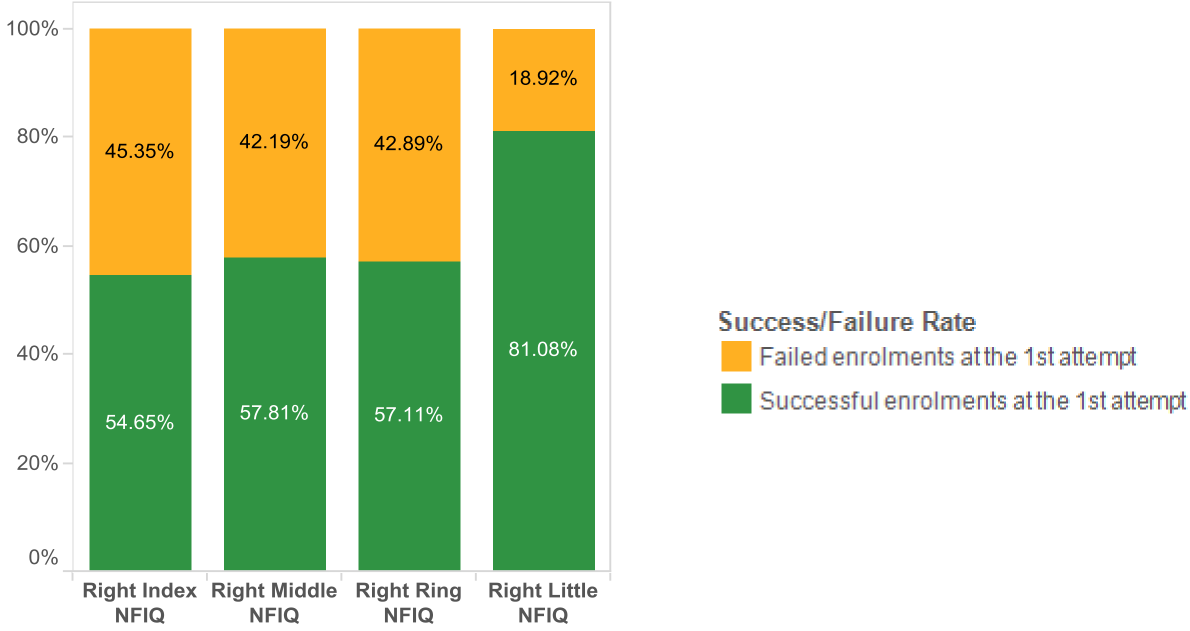


Figure 19 *TC1 Vaalimaa land border - Results of successful and failed enrolments at the first attempt*

3.3.1.4 Schiphol

At Schiphol Airport, the threshold was based on NFIQ with the following values:

- For the little finger: NFIQ score of 4 or better;
- For the thumb, index, middle and ring fingers: NFIQ scores of 3 or better.

The graph below presents the success rate of fingerprint capture for each finger.

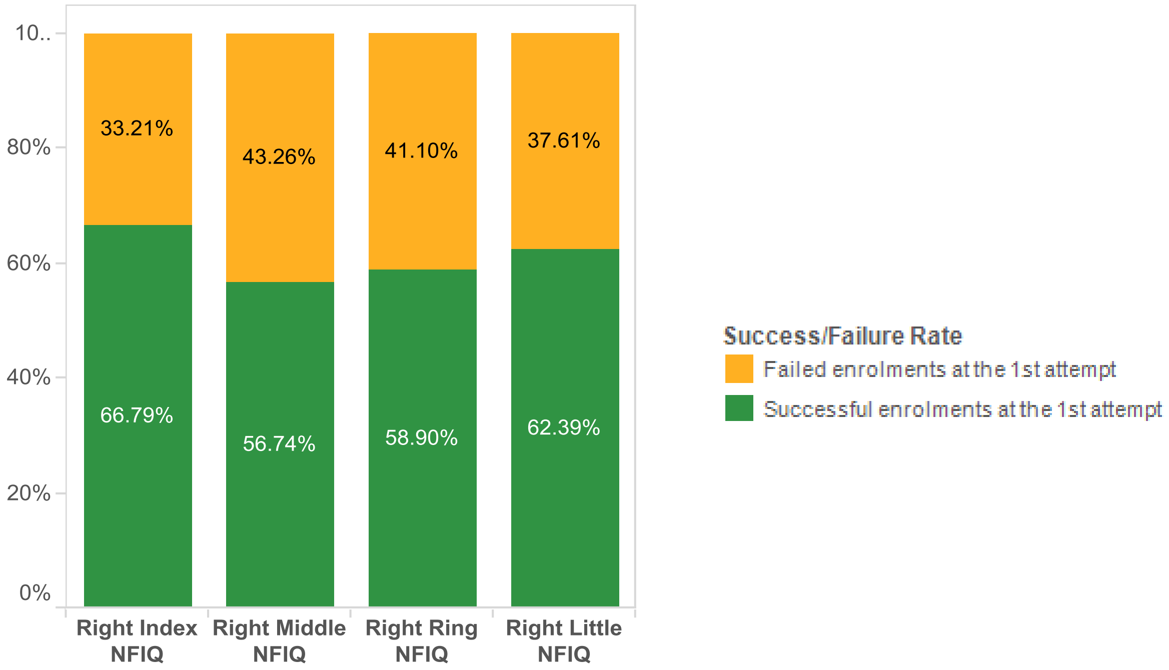


***Figure 20** TC1 Schiphol airport - Results of successful and failed enrolments at the first attempt*

3.3.2 Quality

3.3.2.1 Helsinki

Quality measurement of individual FPs for TC1 in Helsinki was based on:

- NFIQv1;
- Vendor specific index;
- Number of minutiae.

Percentages of NFIQ score occurrences per each finger are presented in the figure below. The results show that the middle finger got an excellent quality score more often than other fingers, whereas the little finger got a poor quality score more often than other fingers. NFIQ's five levels of quality are intended to be predictive of the relative performance of a minutiae-based fingerprint matching system, however no strong correlation – if at all – was observed between the two indicators.

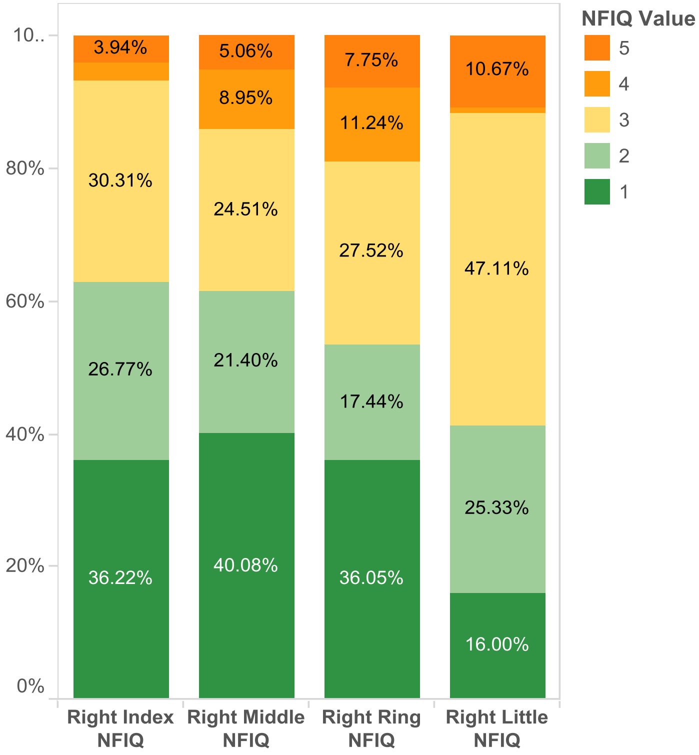


***Figure 21** TC1 Helsinki seaport - Percentages of NFIQ score occurrences per each finger*

The vendor-specific index for FP quality measurement that was applied in Helsinki is based on NIST and highly correlates with the number of minutiae, as presented in the figure below. Values of the index were bulked into the following ranges:

- Below low threshold;
- Between low and medium thresholds;
- Between medium and high thresholds;
- Above high threshold.

The results of fingerprints quality measurement based on a vendor-specific index for the 1st attempt are provided in the table and figure below. Only 1st attempt results are provided, as these are least biased and provide a full picture of the quality measurement. The results show that the better scores were recorded for the middle finger, whereas the scores for the little finger were poorer than for the other fingers.

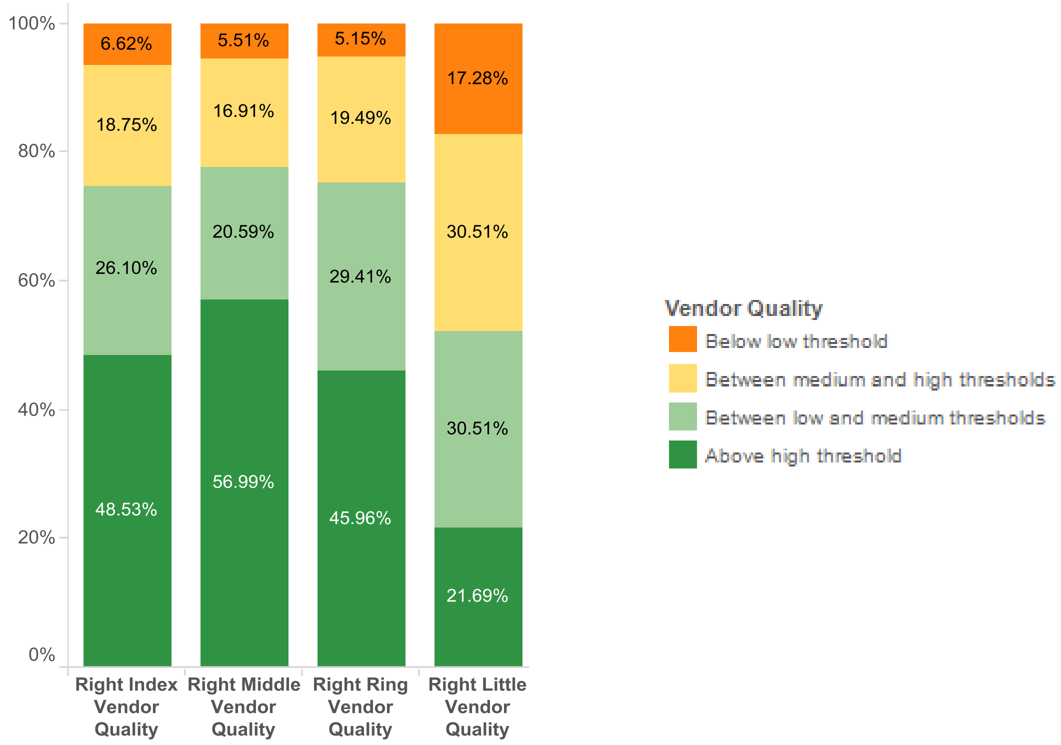


Figure 22 *TC1 Helsinki seaport - Percentages of number of occurrences in different ranges of vendor specific index*

3.3.2.2 Kipoi

The measurement of FP quality relied on NFIQ v1, *i.e.* FP samples were ranked on a scale from 1 (excellent) to 5 (poor). The results of NFIQ score measurement per different finger show that the little finger rarely got an excellent score, *i.e.* only in 7% of all cases. The results also show that the little finger, as well as the ring finger got poor scores more often than the index or middle finger. Please refer to the figure below for more information on NFIQ score distribution per different fingers.

The number of minutiae was also recorded to complement quality measurement based on NFIQ. The correlation between the two indicators is negative: the higher number of minutiae resulted in a lower, *i.e.* better NFIQ score (1 stands for excellent, 5 – for poor). However, the correlation is poor, as apart from the number of minutiae, NFIQ takes into account other indicators as well.

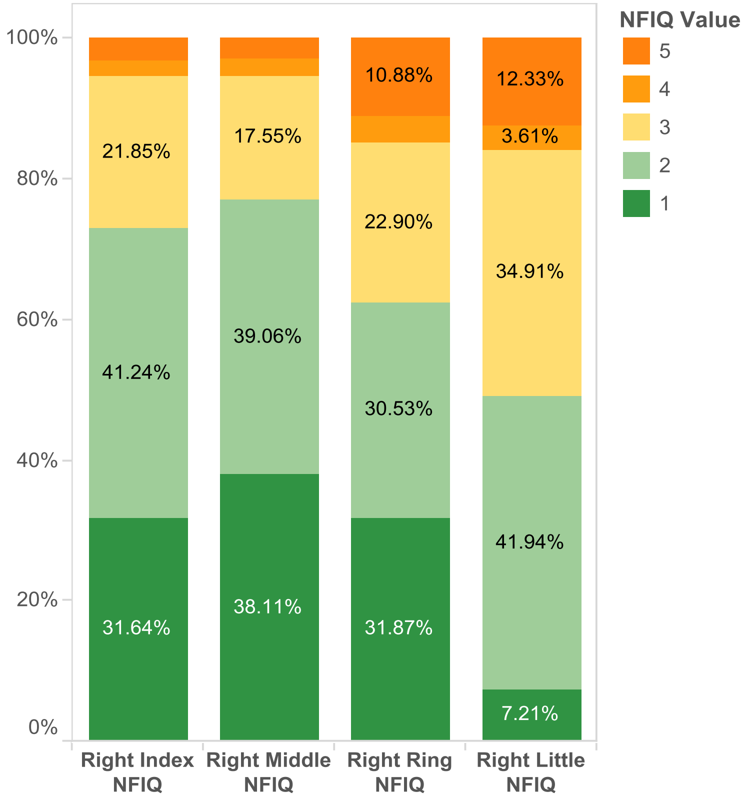


***Figure 23** TC1 Kipoi land border - Percentages of NFIQ score occurrences per each finger*

3.3.2.3 Vaalimaa

FP quality measurement in Vaalimaa was based on the same indicators as in Helsinki:

- NFIQv1;
- Vendor-specific index;
- Number of minutiae.

The results of quality measurement per different finger are provided in the figure below.

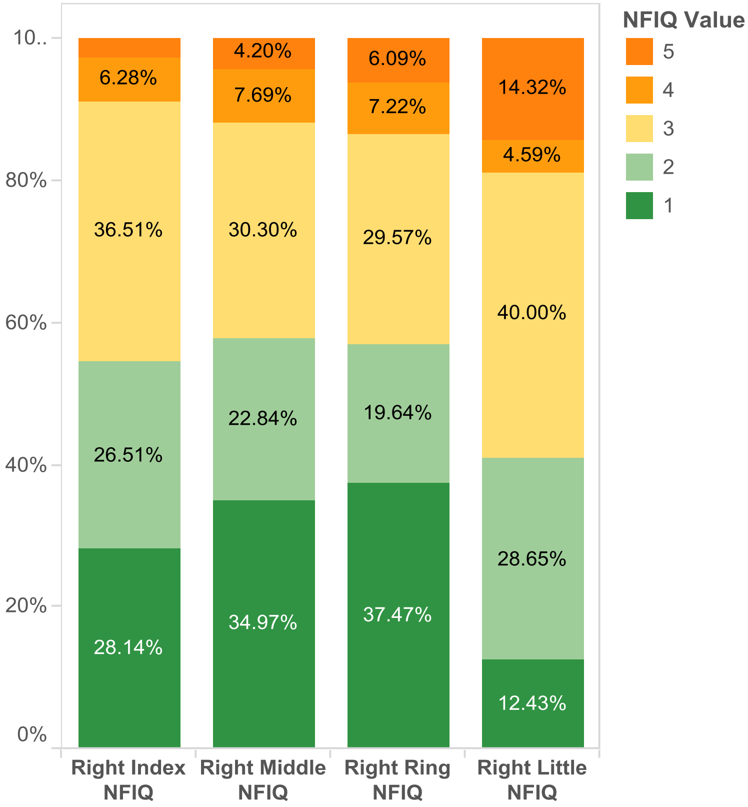


***Figure 24** TC1 Vaalimaa land border - Percentages of NFIQ score occurrences per each finger*

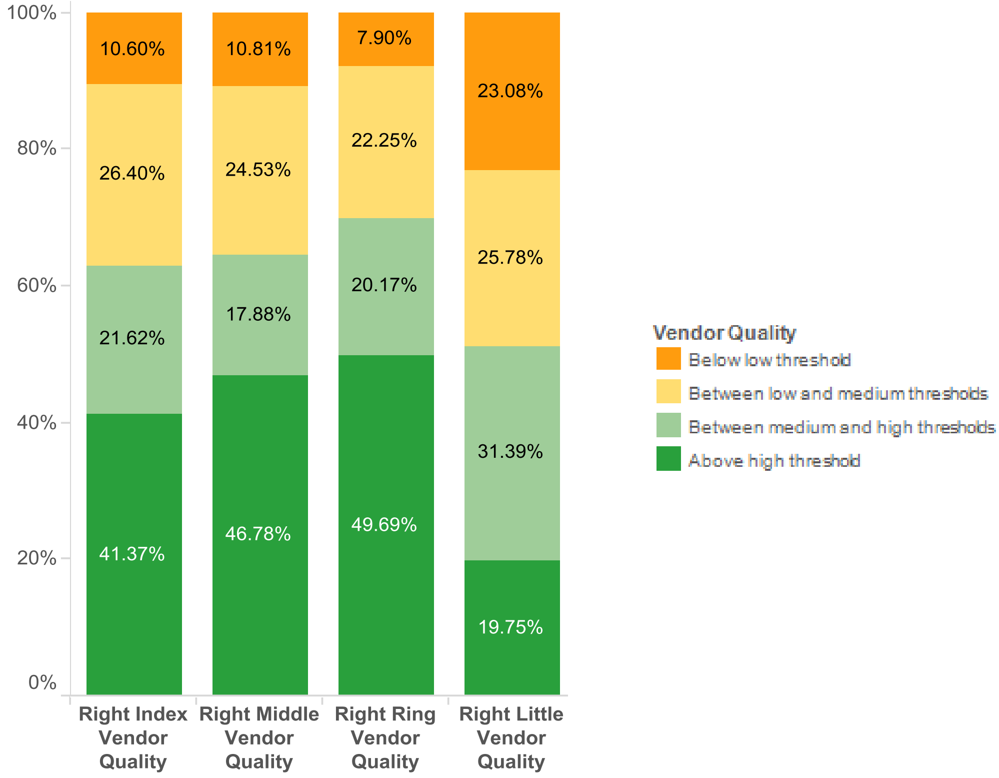


***Figure 25** TC1 Vaalimaa land border - Percentages of number of occurrences in different ranges of vendor-specific index*

3.3.2.4 Schiphol

FP quality measurement in Schiphol for TC1 was based on the following indicators:

- NFIQv1;
- Vendor-specific index;
- Number of minutiae.

The results of quality measurement per different finger are provided in the table and figures below.

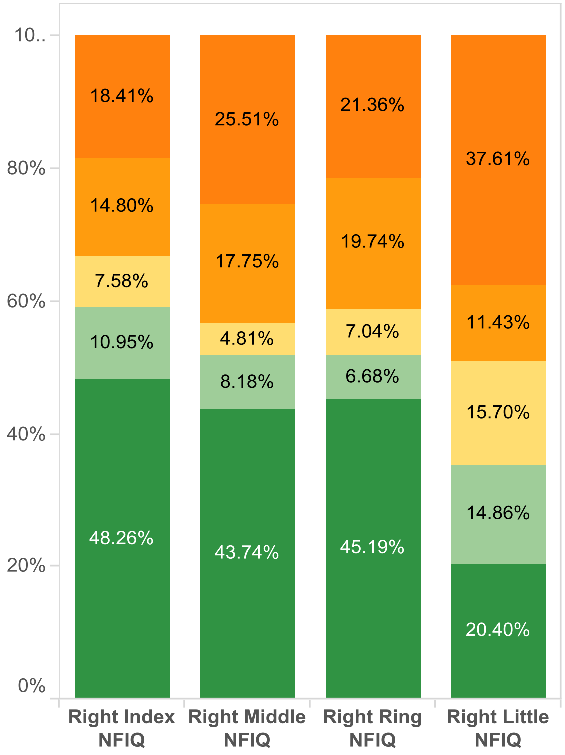


Figure 26 TC1 Schiphol airport - Percentages of number of occurrences in different ranges of NFIQ

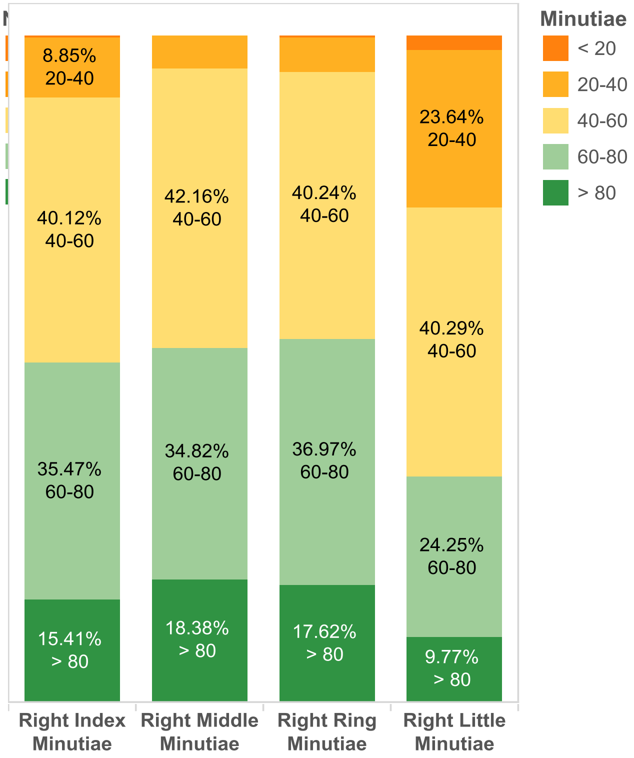


Figure 27 TC1 Schiphol airport - Percentages of number of occurrences in different ranges of minutiae

3.3.3 Duration

The duration of fingerprint enrolment is measured in order to assess the added duration compared to the current situation where no biometric identifier is enrolled. Time-stamped log files, produced by FP scanners, were used for duration measurement.

Measured from ...	**To ...**
The first attempt to capture the FP	The successful capture with a maximum of 3 attempts or the end of the third attempt

3.3.3.1 Helsinki

The time required to enrol 4 FPs with a four-finger slap scanner (index, middle, ring and little finger of the right hand) was 14 seconds on average at entry in the port of Helsinki: However, the longest time it took to enrol 4 FPs was 92 seconds.

Successful enrolment was:

- In 95% of cases less than 20 seconds;
- In 97% of cases less than 30 seconds.

Distribution of duration measurement data of FP enrolment is presented in the table and figure below[11].

Table 8 *TC1 Helsinki seaport - Results of FP enrolment duration measurement at entry*

In seconds	Min	Max	Average
Duration of FP enrolment at entry	6	92	14

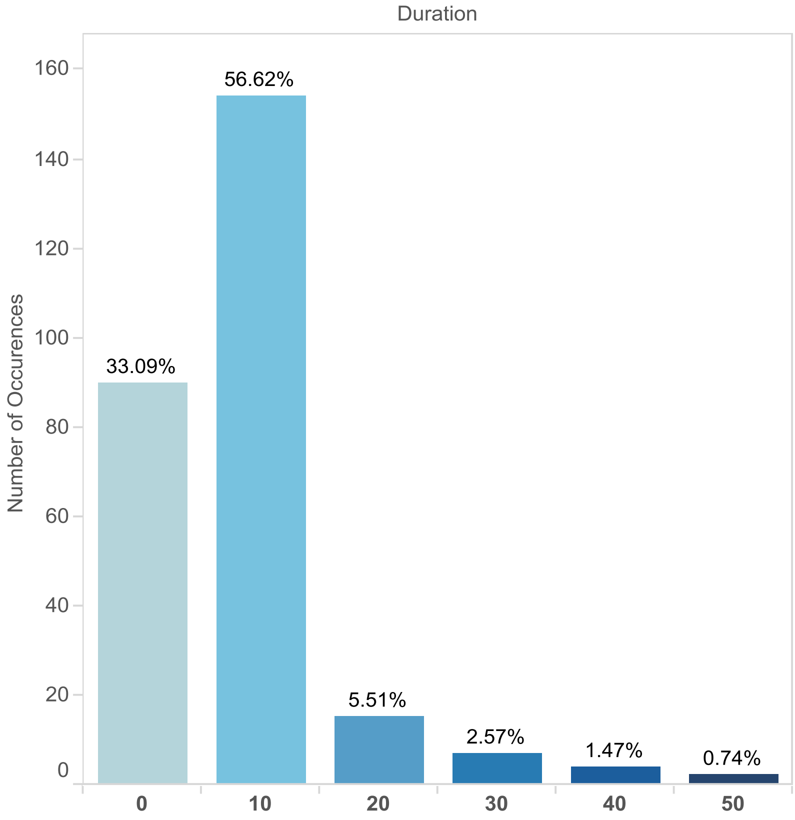


Figure 28 *TC1 Helsinki seaport* ***-*** *Results of the measurement of the duration of 4 FPs enrolment at entry*

3.3.3.2 Kipoi

The minimum duration for the FP enrolment process, measured from the first attempt to capture the FP to the successful capture with a maximum of 3 attempts, amounted to 35 seconds. The enrolment was performed with a portable and handheld two-finger slap scanner, *i.e.* at first, prints of the index and middle fingers were captured and then, prints of the ring and little fingers were captured.

[11] It is important to mention that TC1 was executed in combination with TC4, 6 and 7 in Helsinki which may influence the total duration (although the step is isolated).

The maximum value is not provided, as the upper boundary of 5 minutes was applied to the dataset to remove the extreme values. The median of 126 is significantly less than the mean of 324 in the full dataset, suggesting significant outliers on the right-hand side. Based on the nature of the test and the sample size collected, the central limit theorem would suggest that the data should be normal in shape. Outliers were removed on the right-hand side of the distribution to allow a better fit of data to the normal curve. With a threshold of 5 minutes set at the highest end, this fitting was achieved. This was also consistent with reports from the border guards regarding timings. Within the resulting dataset, the +/- 2 standard deviation of the mean (containing 95% of the data, consistent with our confidence interval usage) runs from 17 seconds to 239 seconds and the majority of the data in the population would seem to fit within this interval.

Distribution of duration measurement data of FP enrolment is presented in the figure below[12].

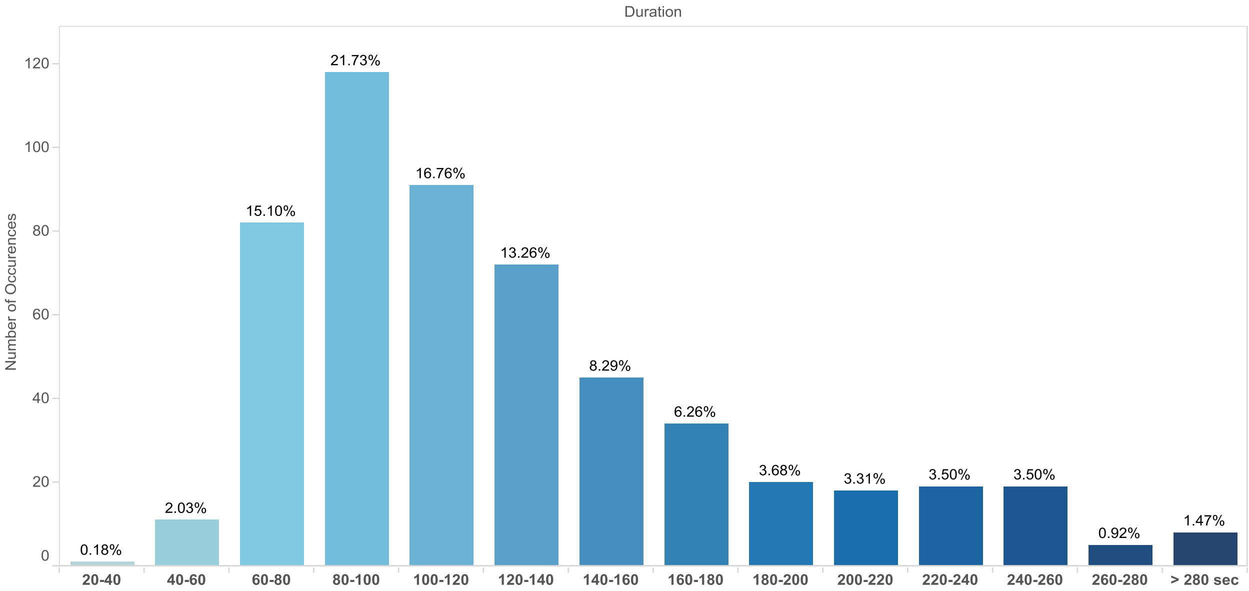


Figure 29 *TC1 Kipoi land border- Results of the measurement of the duration of 4 FP enrolment*

3.3.3.3 Vaalimaa

The average duration of fingerprint enrolment with a four-finger slap scanner (index, middle, ring and little finger of the right hand) at entry amounted to 23 seconds. The maximum duration that was recorded at entry amounted to 94 seconds, whereas the minimum amounted to only 7 seconds.

Successful enrolment represented:

- In 59% of cases less than 20 seconds;
- In 78% of cases less than 30 seconds.

Distribution of duration measurement data of fingerprint enrolment is presented in the table and figure below[13].

Table 9 *TC1 Vaalimaa land border - Results of FP enrolment duration measurement*

[12] It is important to mention that TC1 was executed in combination with TC5 in Kipoi which may influence the total duration (although the step is isolated).

[13] It is important to mention that TC1 was executed in combination with TC4, 6 and 7 in Vaalimaa which may influence the total duration (although the step is isolated).

In seconds	Min	Average	Max
Duration of FP enrolment at entry	7	23	94

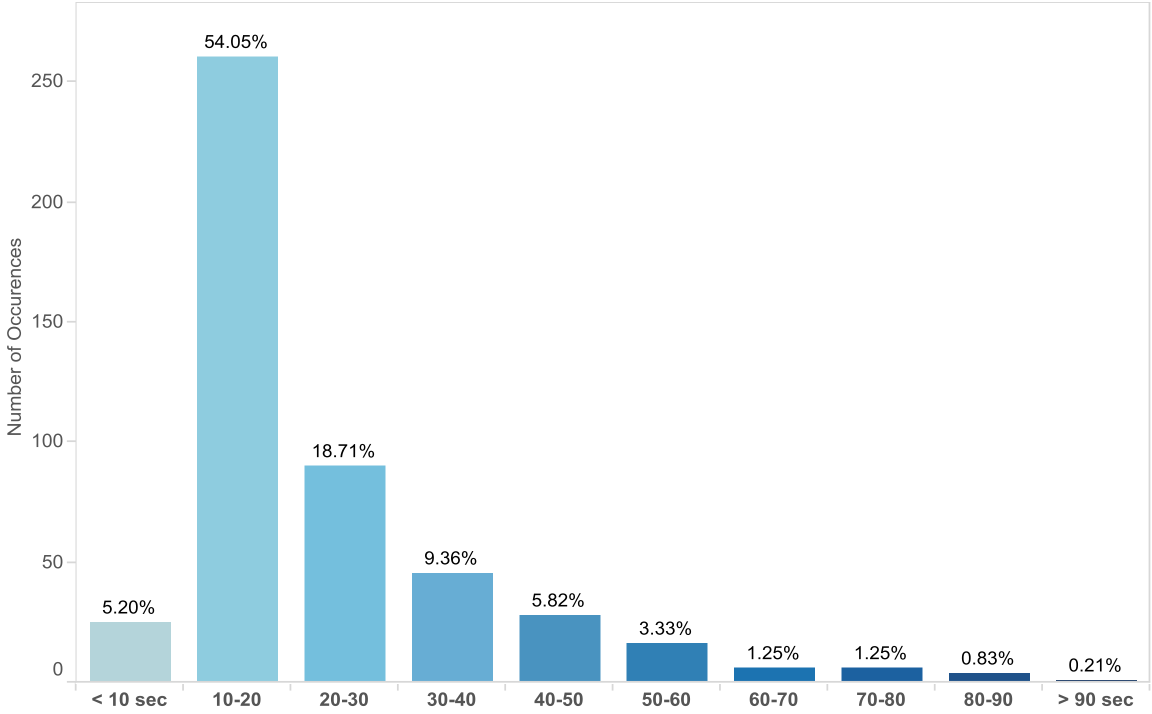


***Figure 30** TC1 Vaalimaa land border- Results of the measurement of the duration of 4 FP enrolment at entry*

3.3.3.4 Schiphol

In Schiphol, the fingerprint capture was performed with a contactless scanner.

The graph below shows that when the enrolment was successful, the fingerprint capture was taking:

- Less than 5 seconds in 38% of cases;
- Less than 20 seconds in 89% of cases;
- More than 30 seconds in 5% of cases.

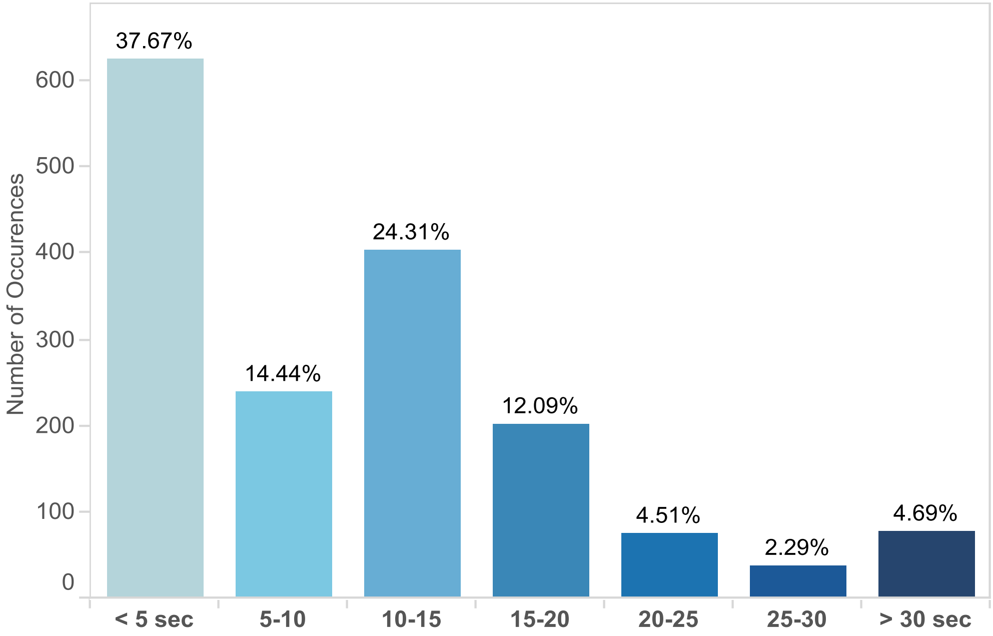


Figure 31 *TC1 Schiphol airport - Results of the measurement of the duration of 4 FP enrolment at entry*

3.4 TC2 Technical and operational questions

3.4.1 Success/failure rate

The success condition is the successful capture of the fingerprint, above a given threshold and within three attempts. The threshold was based on NFIQ with the following values:

- For the little finger: NFIQ score of 3 or better;
- For the ring finger: NFIQ score of 2 of better.

3.4.1.1 Vaalimaa

The results of the successful and failed attempts for each of the fingers of the right and the left hands are provided in the figure below. The data show that the enrolment of the little finger was the most successful in terms of passing the threshold, *i.e.* it succeeded in 89% of the cases in the first attempt for the right hand and also in 85% of the cases in the first attempt of the left hand.

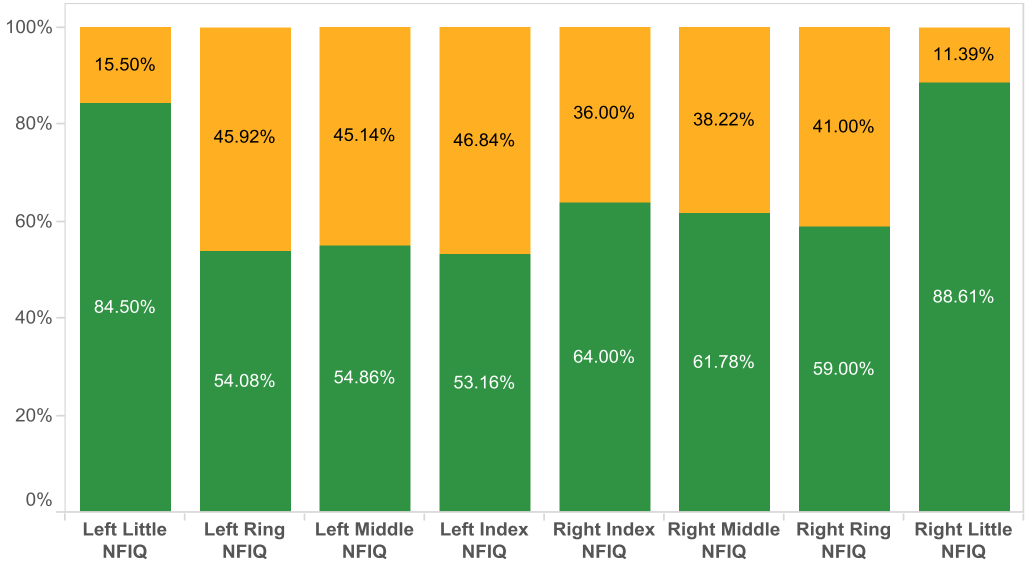


Figure 32 *TC2 Vaalimaa land border - Results of successful and failed enrolments at the first attempt*

3.4.2 Quality

Quality measurement of individual FPs for TC2 in Vaalimaa was based on:

- NFIQv1;
- Vendor-specific index;
- Number of minutiae.

Percentages of NFIQ score occurrences per each finger are presented in the figure below. The results show that the little finger of both hands got a poor quality score more often than other fingers. NFIQ's five levels of quality are intended to be predictive of the relative performance of a minutiae-based fingerprint matching system; however, no correlation was observed between the two indicators.

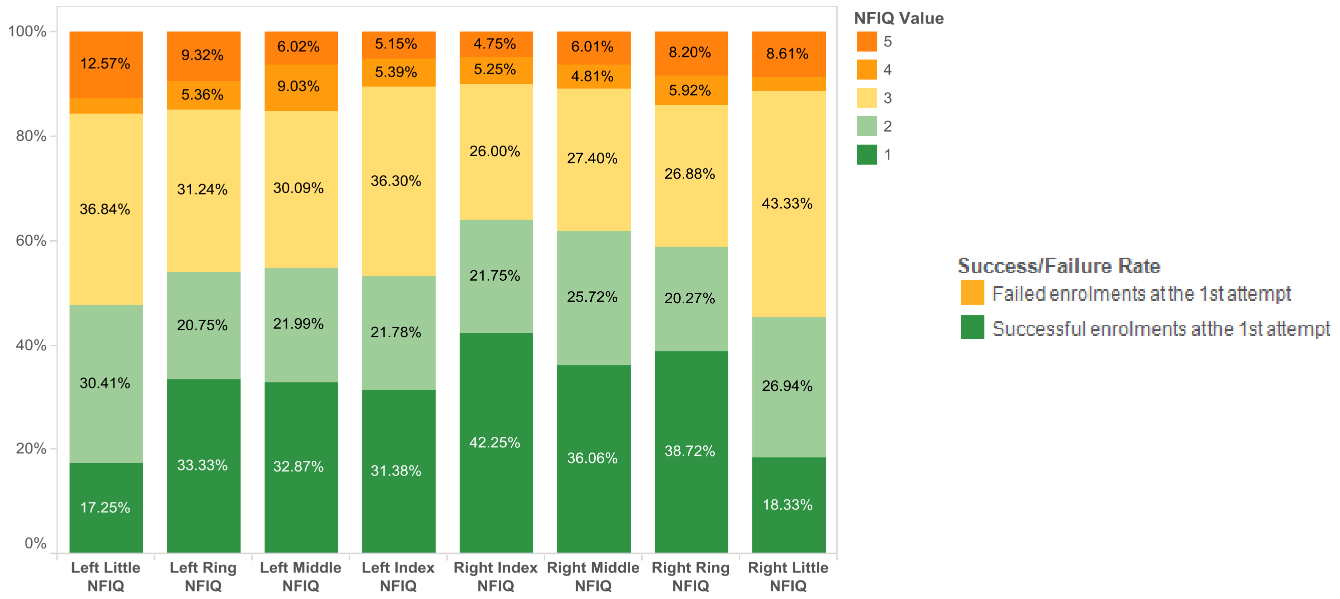


Figure 33 TC2 Vaalimaa land border - Percentages of NFIQ score occurrences per each finger of the right and the left hand

Fingerprint quality measurement for TC2 in Vaalimaa was based on the same indicators as for TC1:

- NFIQv1;
- Vendor-specific index;
- Number of minutiae.

The results of quality measurement per different finger are provided in the figure below.

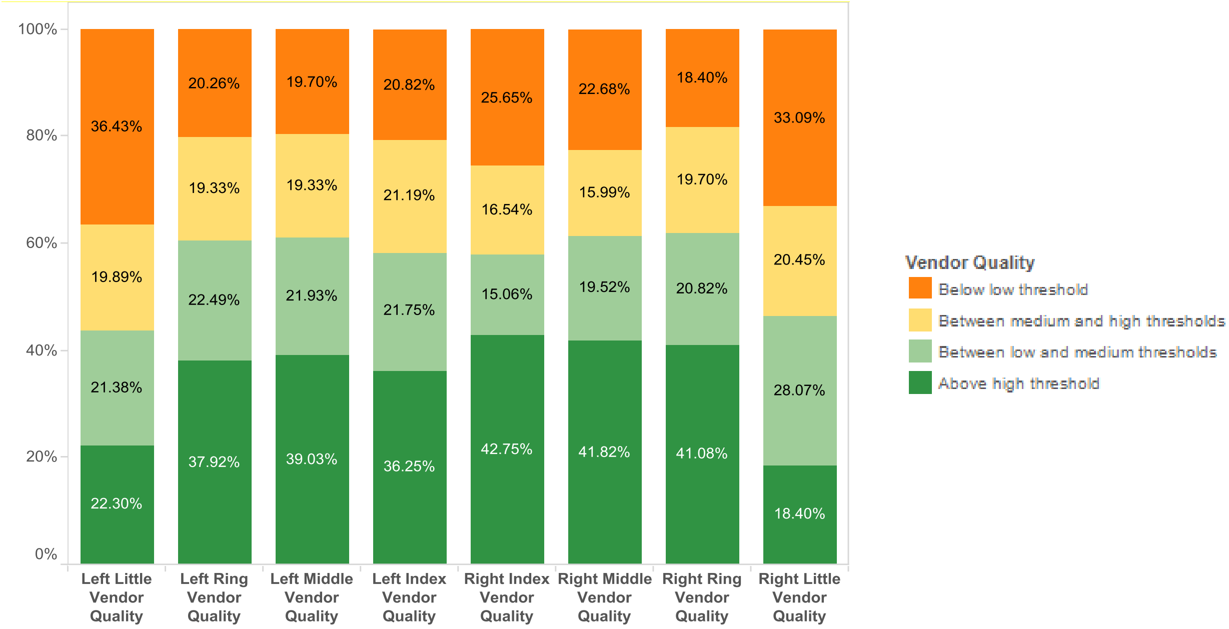


Figure 34 TC2 Vaalimaa land border - Percentages of number of occurrences in different ranges of vendor-specific index

3.4.3 Duration

[Data to be added in the Final Report]

The duration of fingerprint enrolment is measured in order to assess the added duration compared to the current situation where no biometric identifier is enrolled. Time-stamped log files, produced by FP scanners, were used for duration measurement.

Measured from …	**To …**
The first attempt to capture the FP	The successful capture with a maximum of 3 attempts or the end of the third attempt

3.5 TC3 Technical and operational questions

3.5.1 Success/failure rate

The success condition is the successful capture of the fingerprint, above a given threshold and within three attempts.

3.5.1.1 Schiphol

At Schiphol Airport, the threshold was based on NFIQ with the following values:

- For the little finger: NFIQ score of 4 or better;
- For the ring finger: NFIQ score of 3 of better;
- For the thumb, index and middle fingers: NFIQ scores of 2 or better.

The graph below presents the success rate of fingerprint capture for each finger.

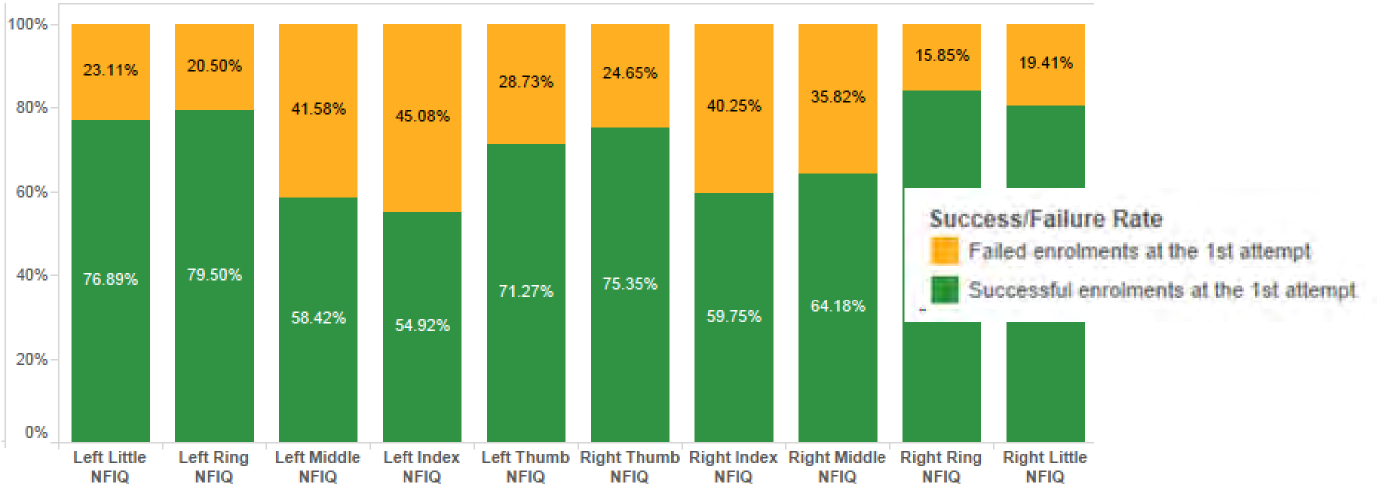


Figure 35 *TC3 Schiphol airport - Results of successful and failed enrolments at the first attempt*

3.5.2 Quality

3.5.2.1 Schiphol

FP quality measurement in Schiphol for TC3 was based on the following indicators:

- NFIQv1;
- Number of minutiae.

The results of quality measurement per different finger are provided in the figures below.

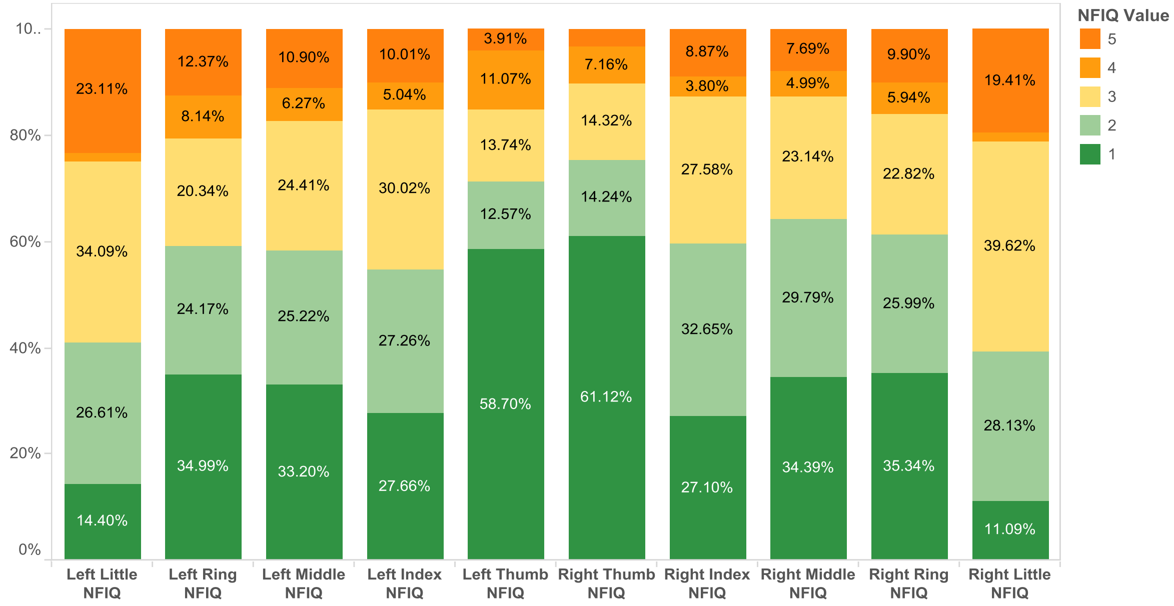


Figure 36 *TC3 Schiphol airport - Percentages of number of occurrences in different ranges of NFIQ*

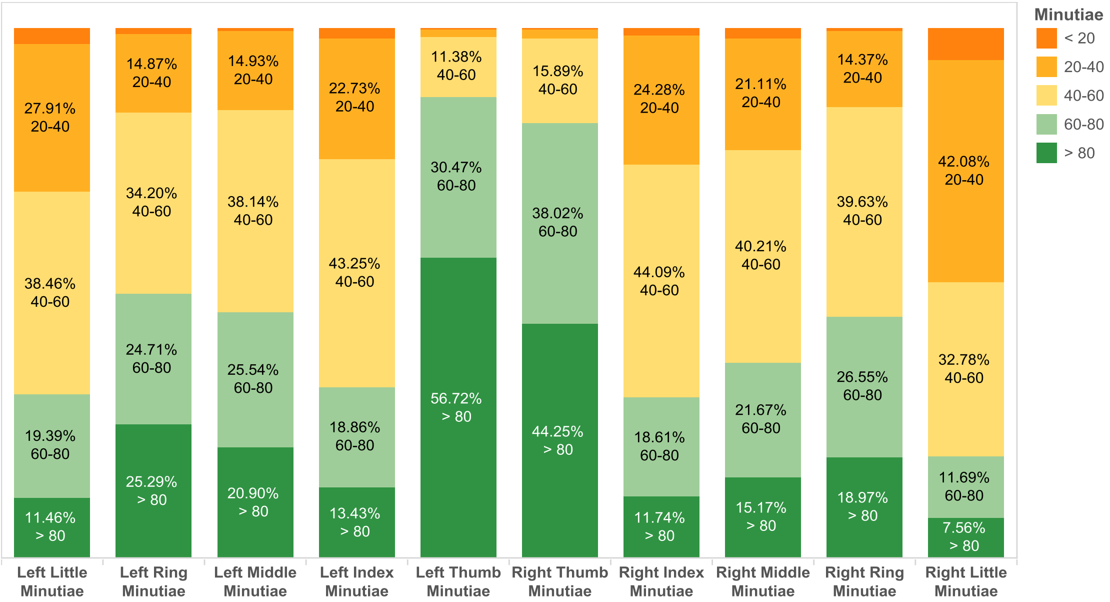


Figure 37 *TC3 Schiphol airport - Percentages of number of occurrences in different ranges of minutiae*

3.5.3 Duration

The duration of fingerprint enrolment is measured in order to assess the added duration compared to the current situation where no biometric identifier is enrolled. Time-stamped log files, produced by FP scanners, were used for duration measurement.

Measured from ...	**To ...**
The first attempt to capture the FP	The successful capture with a maximum of 3 attempts or the end of the third attempt

In Schiphol, the fingerprint capture was performed with a contact scanner.

The graph below shows that when the enrolment was successful, the fingerprint capture was taking:

- Less than 30 seconds in 33% of cases;
- Less than 60 seconds in 81% of cases;
- More than 100 seconds in 5% of cases.

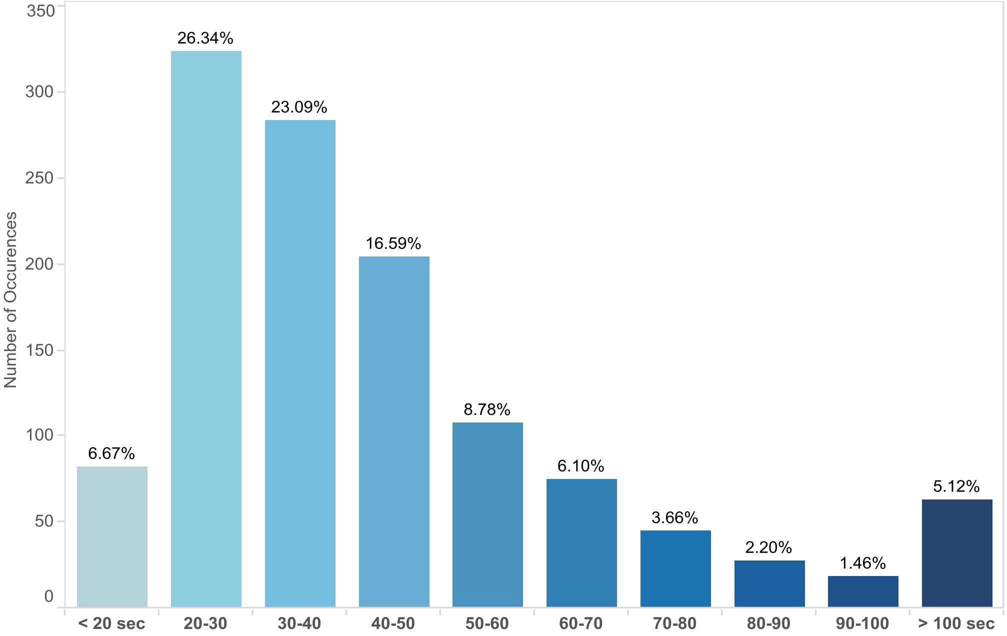


Figure 38 *TC3 Schiphol airport -Results of the measurement of the duration of 10 FP enrolment at entry*

3.6 TC1 Users' feedback

3.6.1 Border guards' feedback

3.6.1.1 Kipoi

In Kipoi land border 4 **border guards** participated and replied to the survey.

The following dashboard presents a summary of replies[14].

Overall feedback[15] ★

Border Guard		Traveller
All 4 did not see any added-value in the process	3 out 4 highlighted the delay of FP reader	Acceptance of travellers was assessed as bad by 3 out of 4 of the border guards[16]

[14] Percentages are calculated per question and are based on the number of replies given. In some cases, BGs have given more than one reply to one question.

[15] Rating : 3 * = good / 2* = neutral / 1* = weak

Potential improvement points

Border Guard		Traveller
Replies indicate that the low speed of equipment causes delays in the process	50 % of replies indicate that equipment could be more ergonomic	60% of replies indicate that more guidance to travellers could improve the process

Potential show-stoppers

Traveller	
Language 44%	Difficulty to use 22%
Long queuing time 22%	Hardware problem 11%

Observations and preliminary conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- **Human factor** and **communication** are paramount:
  - More guidance to travellers would improve the process;
  - Language barrier is an important show-stopper since lots of TCNs (in this case mainly Turkish travellers) do not speak neither English nor Greek.
- **Equipment speed could be improved**:
  - Slowness of the FP reader causes delays in the process (as explained in chapter 3);
  - Some participants refused to participate because of the queuing time.

3.6.1.2 Vaalimaa

In Vaalimaa land border, **4 border guards** participated and replied to the survey.

The following dashboard presents a summary of replies[17].

Overall feedback[18] ★ ★

Border Guard		Traveller

[16] This is not aligned with score of travellers' survey: 82.3% are satisfied or very satisfied. In some cases, BG indicated several answers.

[17] Percentages are calculated per question and are based on the number of replies given.

[18] Rating : 3 * = good / 2* = neutral / 1* = weak

2 out of 4 felt more confident with the equipment 2 out of 4 did not see any difference with the equipment	2 out of 4 highlighted the slowness of fingerprint reader 1 out of 4 rated the usability as good 1 out of 4 did not express any opinion	Acceptance of travellers was assessed as good by 3 out of 4 of the border guards[19]

Potential improvement points

Border Guard		Traveller
Replies indicate that FP reader should be faster	20% of replies indicate that equipment could be more ergonomic	80% of replies indicate that more guidance to travellers could improve the process

Potential show-stoppers

Traveller	
Language 29%	Hardware problem 14%
Longer queuing time and the use of a camera in parallel have been identified as an issue for some travellers in 29% of replies	Difficulty to use 14%
	-

Observations and preliminary conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- **Human factor** and **communication** are paramount:
  - Difficulty to communicate with some TCNs (language barrier as travellers are mainly Russian citizens speaking neither FI nor EN) caused abortion of tests in some cases;
  - Some travellers refused to participate because of the use of a camera in parallel.
- **Equipment speed could be improved**:
  - Some travellers refused to participate because the enrolment lasted too long;
  - FP reader is sometimes not easy to use (as explained in chapter 3).

3.6.1.3 Helsinki

In Helsinki sea border, **2 border guards** participated and replied to the survey.

The following dashboard presents a summary of replies[20].

Overall feedback[21] ★ ★

[19] This is aligned with score of travellers' survey: 90.3% are satisfied or very satisfied.

[20] Percentages are calculated per question and are based on the number of replies given. In some cases, BG indicated several answers.

[21] Rating : 3 * = good / 2* = neutral / 1* =weak

Border Guard		Traveller
They both felt more confident with equipment	They both rated the usability of equipment as good	They both indicated that travellers were mostly enthusiastic[22]

Potential improvement points

Border Guard		Traveller
Replies indicate that too many verbal instructions are needed to ensure success	The interaction equipment-traveller should be improved: e.g. indication of real-time performance – more visual representation –would help travellers in the process (position for FP and FI taking should be indicated)	

Potential show-stoppers

Traveller	
Language: Russian interpret is necessary	Difficulty to use: not enough indication to travellers
Many travellers tend to be suspicious about the use of their fingerprints	-
	-

Observations and preliminary conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- **Equipment seems reliable:**
  - Software is easy to use.

- **Difficulties experienced with equipment:**
  - More real-time indication/feedback to travellers (where fingers should be placed) would help the enrolment would ease the process and lower instructions from border guards;
  - Usually the little finger is out of the reading area;
  - Large hands can be problematic, as well as dry fingers (BGs suggested to provide moisturizing pads to travellers).

3.6.2 Travellers' feedback

After the testing, travellers were asked to evaluate their experience on a scale from very unsatisfied to very satisfied, using either the survey tablet or the survey integrated in the device. Overall, the feedback was very

[22] This is aligned with travellers' survey feedback showing 82.5 % of satisfied or very satisfied answers for TC 1.

positive, yet it is important to mention that TC1 was executed in combination with other TCs at the majority of BCPs, thus this reflects several TCs, rather than only the enrolment of FPs.

3.6.2.1 Helsinki

TC1 is executed together with TC4 (FI enrolment), TC6 (FI capturing from e-MRTD) or TC7 (verification of live FI against FI captured from e-MRTD) in Helsinki, thus combined travellers' feedback is given, which reflects the assessment of all TCs. The results show that the majority of travellers were either very satisfied or satisfied about participation in ed or very unsatisfied.

Please refer to the figu

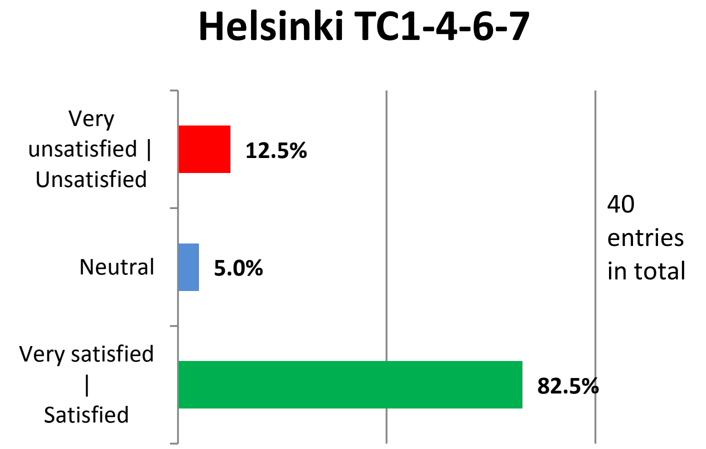


***Figure 39** TC1, 4, 6 and 7 Helsinki seaport - Results of travellers' feedback*[23]

3.6.2.2 Kipoi

Enrolment of 4 FPs is executed together with iris enrolment in Kipoi, thus travellers' feedback reflects both TCs. Overall, travellers expressed satisfaction with the participation in the Pilot or remained neutral. Negative feedback is provided b provided in the figure below.

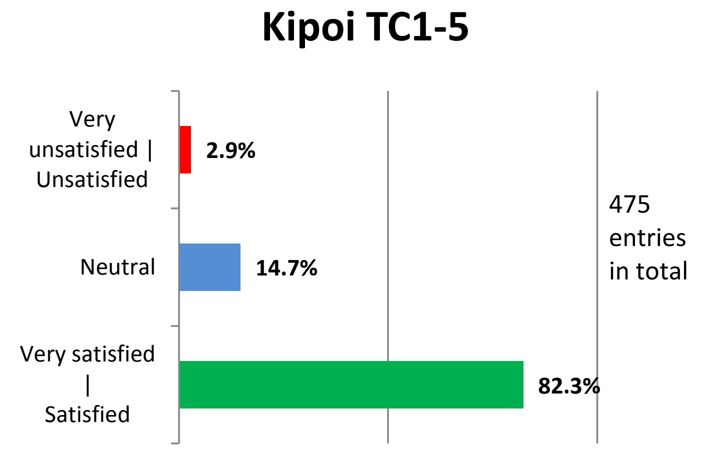


***Figure 40** TC1 and 5 Kipoi land border - Results of travellers' feedback*

[23] It is important to note that due to technical issues, the survey collection has been discontinued and a low number of entries for travellers' feedback have been recorded.

3.6.2.3 Vaalimaa

A great majority (over 90%) of travellers who participated in the Pilot in Vaalimaa were either satisfied or very satisfied; however, this feedback was given not only for TC1 execution, but also TC4 (FI enrolment), TC6 (FI capturing from e-MRTD) which were carried out in parallel. Please ref

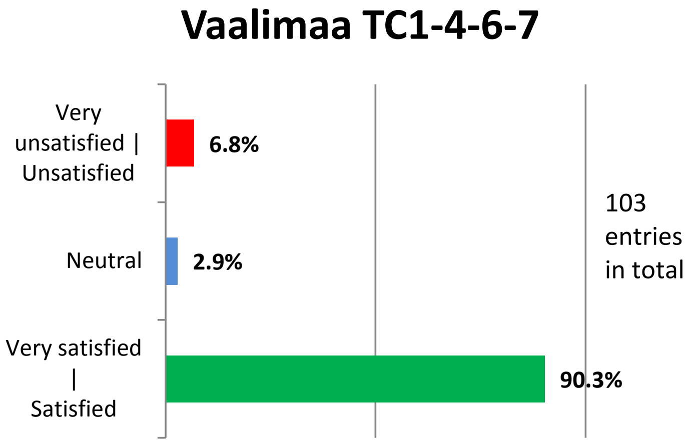


Figure 41 *TC1, 4, 6 and 7 Vaalimaa land border - Results of travellers' feedback*

3.6.2.4 Schiphol

A majority (over 75%) of travellers who participated in the tests for TC1 in Schiphol were either satisfied or very satisfied. On th e unsatisfied or very unsatisfied.

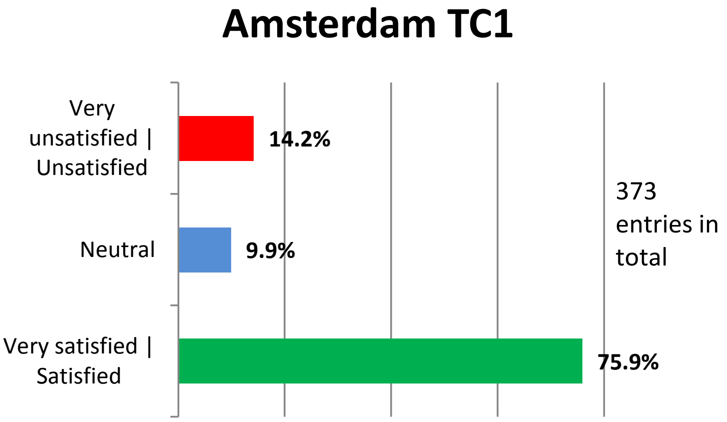


Figure 42 *TC1 Schiphol airport - Results of travellers' feedback*

3.7 TC2 Users' feedback

3.7.1 Border guards' feedback

In Vaalimaa land border, **2 border guards** participated and replied to the survey.

The following dashboard presents a summary of replies[24].

Overall feedback[25] ★

Border Guard		Traveller
- 1 BG did not see any difference with the equipment -1 BG did not see any added-value for this type of BCP (8 FP taking too long although application is easy to use)	- 1 BG rated the usability as bad given time needed to perform - 1 BG highlighted the instability of fingerprint reader	2 BGs assessed acceptance of traveller as good[26] with the caveat that if the operation has to be repeated, it could be experienced as too lengthy for passengers

Potential improvement points

Border Guard		Traveller
Replies indicate that the enrolment of 8FPs is time consuming and increase the workload	-1 BG: sidelight disturbs FP reader -1BG: environmental issues such as cold fingers, dry fingers, cold glass have negative impact on equipment	2 BGs agreed that more guidance to travellers could improve the process

Potential show-stoppers

Traveller	
-	Hardware problems have been identified by both BGs
Long enrolment time and the use of a camera in parallel have been identified as an issue for some travellers	-
	-

Observations and preliminary conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

[24] Percentages are calculated per question and are based on the number of replies given. In some cases, BGs have given more than one reply to one question.

[25] Rating : 3 * = good / 2* = neutral / 1* = weak

[26] This is aligned with score of travellers' survey: 91.2% are satisfied or very satisfied.

- **Environmental conditions play an important role**: cold weather conditions are not ideal for device (as explained in chapter 3);
- **No value-added of taking 8 FPs at land border:** process is too lengthy (as explained in chapter 3).

3.7.2 Travellers' feedback

TC2 is executed together with TC4 (Enrol live facial image), 6 (Capture facial image from e-MRTD) and 7 (Verify facial image captured from e-MRTD against the Live facial image) in Vaalimaa, thus combined travellers' feedback is given which reflects the assessment of all TCs. The results show that a large majority of travellers were either very satisfied or satisfied with the participation in the experiment. Less than four percent of the travellers rep ure below for more details.

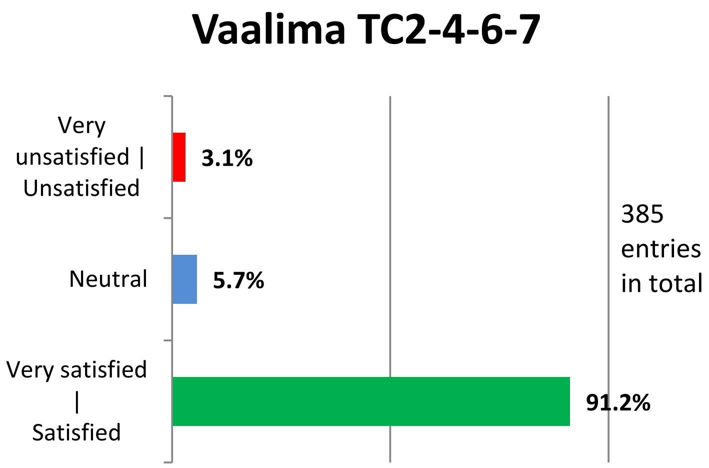


Figure 43 *TC2, 4, 6 and 7 Vaalimaa land border- Results of travellers' feedback*

3.8 TC3 Users' feedback

3.8.1 Border guards' feedback

[Data not collected as of 25 June to be added for Final Report]

3.8.2 Travellers' feedback

A majority (over 80%) of travellers who participated in the tests for TC1 in Schiphol were either satisfied or very satisfied. On the other hand, around 10% of participants reported that they were unsatisfied or very unsatisfied.

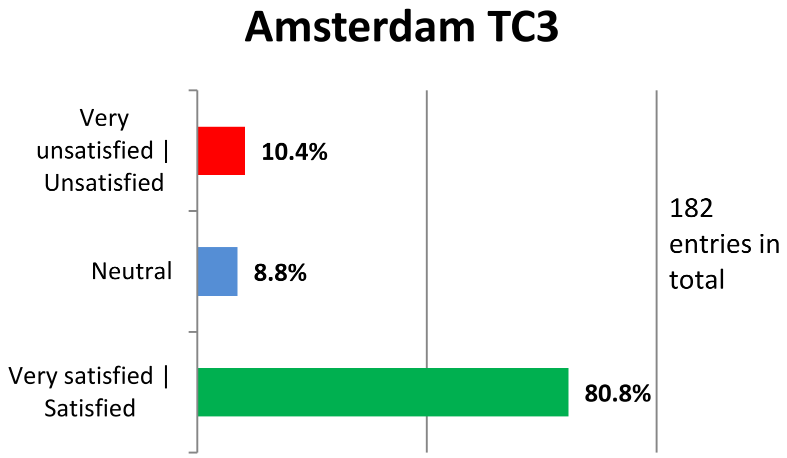


Figure 44 *TC3 Schiphol airport- Results of travellers' feedback*

3.9 Constraints

[To be added in the Final Report]

3.10 Feasibility

[To be added in the Final Report]

4. Facial image

4.1 Introduction

[Treatment and cleaning of the data to be finalised for Final Report]

The facial image is the most commonly used biometric modality in current border control processes across Schengen territory. It has been used to verify identity at the border for decades, first as a printed picture attached to the passport, and now also stored digitally on the chip. It is now also used in more automated ways at both ABC gates and kiosks.

Its proven reliability and ease of use were considered when selecting facial image as a biometric identifier option for EES in the Technical Study. Indeed it is accessible in a non-contact manner, quickly and easily without dependence on travellers being accustomed to an unusual enrolment procedure. Also, it is the only biometric readily available on most documents, meaning that a reference biometric is available to tie the traveller to their document, unlike for any other biometric. The facial image was considered as being part of the individual file of a traveller and for "local" verification (*i.e.* bearer verification) where the facial image of the e-MRTD would be compared with a live image of the traveller, when arriving at the border control.

During operational testing within the Smart Borders Pilot, tests were executed that focussed on operational processes taking place at the border:

- Enrolment of a live facial image from the traveller;
- Capture of the facial image from the e-MRTD;
- Verification of one against the other.

The objectives of the tests are outlined at the beginning of this chapter. In subsequent sections, a description of the methodology and conditions in which the tests were performed is provided, and indicators needed to help assess the feasibility of using facial image as a biometric identifier in the context of border checks are presented.

4.1.1 Objective

Three Test Cases have been executed that relate to the use of the facial image in border checks:

1. **Capture facial image from e-MRTD (TC6) –** evaluate the feasibility, user-acceptance, timing and the delivered quality of enrolling the photo contained in the e-MRTDs of TCNs at each type of border crossing (air, sea, land) in various conditions.
2. **Enrol live facial image (TC4) –** evaluate the feasibility, user-acceptance, timing and delivered quality of taking live facial images (photos) from TCNs at each type of border crossing (air, sea (cruise ship), land).
3. **Verify facial image captured from e-MRTD against the live facial image (TC7)** – evaluate the feasibility, user-acceptance, duration and the delivered quality of comparing the photo captured from the e-MRTD with the live facial image.

Although TC9 (Automated Exit Checks of TCNs), TC10 (Use of Self-Service kiosks) and TC11 (Pre-border checks at Land Borders) also rely on the facial image as the principal biometric modality, results from these test cases are analysed in more detail in chapters 6 and 7.

4.1.2 Workflow for the combination of the test cases

The process of testing TC6, 4 and 7 together is built upon four steps:

1) Passport Inspection (including Passive Authentication[27]) (first part of TC6);
2) Capture of the facial image from the e-MRTD (located in Data Group 2 of the passport chip[28]) (second part of TC6);
3) Enrolment of a live facial image (TC4);
4) Verification of a facial image from the e-MRTD against a live facial image (TC7).

In some of the tests, the above process will be combined with capturing iris patterns *i.e.* in Cherbourg (FR) and Iasi (RO). The result of testing iris pattern enrolment is described in chapter 5.

4.2 Methodology

The objectives of the Test Cases are addressed in order to cover the following matters for which operational testing results would be beneficial for future decision making.

1. **Operational and technical questions per type of BCP (air, sea, train, road, moving train, moving vessel)**
   a. Success/failure: What is the success/failure ratio for the different steps of the process?
   b. Quality of the enrolment/capture: What is the recorded quality?
   c. Duration: What is the process duration of the new process and how does it compare to existing processes in place at the various borders? What is the added duration for Passive Authentication? Can the Live facial image and the e-MRTD facial image be captured at the same time?
   d. Security: What does the need to perform Passive Authentication add to the complexity of the set-up?
2. **Users' feedback**
   a. Perception of TCNs: What is the traveller's perception of the border control process?
   b. Feedback from Border Guards: How do border guards experience the changes made to the border control process?
3. **Constraints:** Which environmental constraints influence the quality of the biometrics (facial image) and the duration of the process?
4. **Feasibility:** Can the processes outlined in the Test Cases be applied at all types of borders? This question will be answered on the basis of the findings of the questions above.

4.2.1 Methodology by TC

The facial image test cases have been analysed using both the results of operational testing and the findings of desk research.

Each TC is first analysed independently, and later TCs 6, 4 and 7 are summarised to present the indicators for the whole process.

For TC6, indicators from the field are complemented by evidence from desk research on the feasibility of checking passport integrity (using Passive Authentication) and capturing the facial image (from DG2) and possible issues in this regard.

[27] "Passive Authentication" (PA) is used to check if the data on the RF chip of the electronic ID document is authentic and unforged. For more information, please refer to Appendix 10.4 **Error! Reference source not found.**

[28] For more information about the logical data structure of eMRTDs, please refer to Appendix 10.4.1 E-MRTD chip data structure

For TC4, results from the field are the basis of most information. A potential accelerator of the process is also identified and presented through desk research and operational findings.

For TC7, indicators from the field are the sole source of information.

For the summary, indicators from the field are complemented by desk research on the constraints brought by the Passive Authentication.

4.2.2 BCP selection

Facial image Test Cases will be carried out at the following ten BCPs.

Air

- Arlanda (SE)
- Madrid (ES)
- Charles de Gaulle (FR)

Sea

- Helsinki (FI)
- Genoa (IT)
- Cherbourg (FR)

Land

- Vaalimaa (FI)
- Sculeni (RO)

Moving Train

- Iasi (RO)

Moving Vessel

- Piraeus (EL)

This interim report only gives an insight into the preliminary data gathered from Madrid.

4.2.3 Type of equipment

4.2.3.1 Capture of e-MRTD facial image (including Passive Authentication)

Devices for the reading of e-MRTDs vary within the following categories.

***Table 10** Categories of devices for the reading of e-MRTDs*

Mobile or fixed solution	**Fixed:** Requires a connection to a fixed element. **Mobile solution:** Can be freely transported and operated.
Swipe or full page MRZ scanner	**Swipe:** Requires the border guard to swipe the document against a reading band to capture the MRZ. Reading the chip must then take place in another step. **Full page:** Allows the border guard to place and hold the document on a scanning surface, while the chip is read.

4.2.3.2 Enrolment of live facial image

Cameras for the enrolment of a live facial image vary within the following categories.

***Table 11** Categories of devices for the live facial image enrolment*

Mobile or fixed solution	**Fixed:** Requires a connection to a fixed element. **Adjustable fixed**: Can be slightly repositioned by the Border Guard, to adapt to the subject to be enrolled. **Movable fixed**: Can be deployed in various places with little effort, but needs to remain fixed during operation. **Mobile solution:** Can be freely transported and operated without space limitation.
Individual shots or continuous video capture	**Camera shots:** Live image captures are attempted one by one. **Continuous video:** Images are extracted from a continuous video capture until a picture of sufficient quality is captured.

Integrated lighting system	**Yes**: Built-in flash/LED system helping to achieve correct lighting conditions on the subject of enrolment. **No**: No lighting system; requires a more controlled lighting environment.
Iris capability[29]	**Yes, simultaneously**: Facial image and iris picture can be taken at the same time. **Yes, not simultaneously:** Facial image and iris picture can be taken, but not at the same time or in the same conditions (e.g. the subject should be closer to the camera for iris capture). **No**: The camera cannot enrol an iris pattern image.

4.2.3.3 Verification of live facial image against e-MRTD facial image

Facial image matching systems can vary within the following categories.

Table 12 *Categories of facial image matching system*

Local or central solution	**Local:** Can perform matching locally, using software and processing power integrated in the device. **Central:** Needs to send the images to be matched to a central server, this option requiring connectivity.

4.2.4 Configuration per BCP (Madrid)

4.2.4.1 Overview of equipment used

Test Case 6

Table 13 *TC6 Madrid airport – TC configuration*

Duration of the test	6 weeks (from 27.04.2015 to 08.06.2015)
Timetable of the tests	09:00 – 15:30 adjusted according to traveller flows
Layout	Dedicated manual booth with 2 workstations
Sample size achieved	3203
Technical integration	Integrated
Integration within the regular border crossing process	Integrated
Equipment type	Existing e-MRTD reader, Fixed, Full-page
Enrolment/verification threshold	Threshold set on the verification score against the FI on the e-MRTD, based on a vendor-specific index. Scale 0 to 100. Threshold value set to 30 on a scale of 100, corresponding to a FAR of approximately 0.3%. These are the same settings as the ones used at the operational ABC gates in Madrid used for EU citizens.
Travellers' survey	Survey on eu-LISA tablet
Test personnel	Shifts of 2-3 border guards plus hostess

Test Case 4

Table 14 *TC4 Madrid airport - TC configuration*

[29] For more information on using the iris as a biometric identifier, please refer to the Iris Chapter.

Duration of the test	6 weeks (from 27.04.2015 to 08.06.2015)
Timetable of the tests	09:00 – 15:30 adjusted according to traveller flows
Layout	Dedicated manual booth with 2 workstations
Sample size achieved	3203
Technical integration	Integrated
Integration within the regular border crossing process	Integrated
Equipment type	• New Fixed adjustable Camera; • 1080p; • Auto-focus 10cm-∞; • Continuous video capture; • Lighting system; • No iris capability.
Enrolment/verification threshold	Threshold set on the verification score against the FI on the e-MRTD, based on a vendor-specific index. Scale 0 to 100. Threshold value set to 30 on a scale of 100, corresponding to a FAR of approximately 0.3%. These are the same settings as the ones used at the operational ABC gates in Madrid used for EU citizens.
Travellers' survey	Survey on eu-LISA tablet
Test personnel	Shifts of 2-3 border guards plus hostess

Test Case 7

Table 15 *TC7 Madrid airport - TC configuration*

Duration of the test	6 weeks (from 27.04.2015 to 08.06.2015)
Timetable of the tests	09:00 – 15:30 adjusted according to traveller flows
Layout	Dedicated manual booth with 2 workstations
Sample size achieved	3203
Technical integration	Integrated
Integration within the regular border crossing process	Integrated
Equipment type	New local facial image matching system
Enrolment/verification threshold	Threshold set on the verification score against the FI on the e-MRTD, based on a vendor-specific index. Scale 0 to 100. Threshold value set to 30 on a scale of 100, corresponding to a FAR of approximately 0.3%. These are the same settings as the ones used at the operational ABC gates in Madrid used for EU citizens.
Travellers' survey	Survey on eu-LISA tablet
Test personnel	Shifts of 2-3 border guards plus hostess

4.3 TC6 Technical and operational questions

4.3.1 Success/failure rate

The success condition for TC6 is the successful capture of the image from the e-MRTD.

Furthermore, the main reasons for failure and their frequency are also identified.

The graph below presents the success rate of facial image chip capture from the e-MRTDs of participating TCNs.

While interpretation of error results is still ongoing, it can be observed that when communication with the chip was possible, the capture of the facial image was possible in the majority of cases (76%). The failures were due to passive authentication errors. Due to the low granularity of the error codes, it is not possible to provide more details into the reason for Passive Authentication failures or chip reading errors.

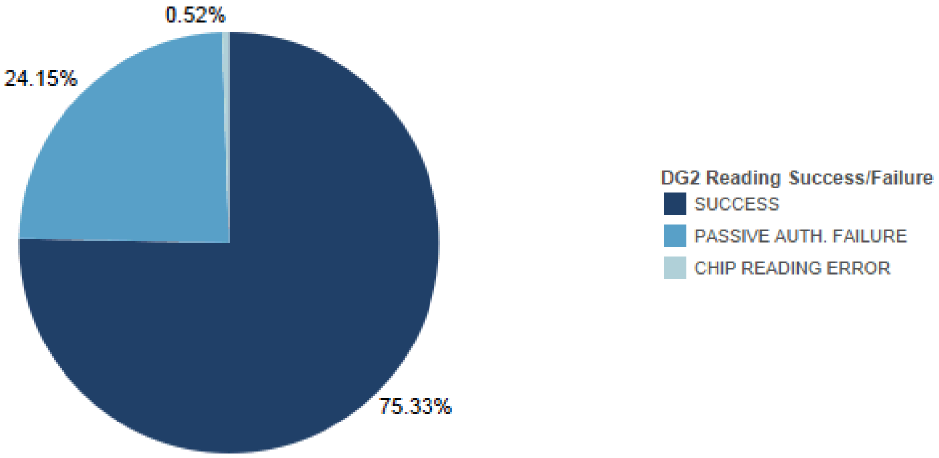


Figure 45 *TC6 Madrid airport - Success/failure ratio for facial image capture from the chip and cause of failure*

4.3.2 Quality

The quality of the facial image captured from the chip is evaluated based on one of two criteria, or both, depending on the data received from the MS:

- ICAO 9303 guidelines (extract);
- Vendor quality index.

The indicator retained for Madrid Airport is the vendor's quality index.

The graph below presents the quality score results for the facial images stored on chips obtained in Madrid. The score is based on the vendor's quality index.

As the graph shows, the majority (more than 99%) of facial images have quality above 80.

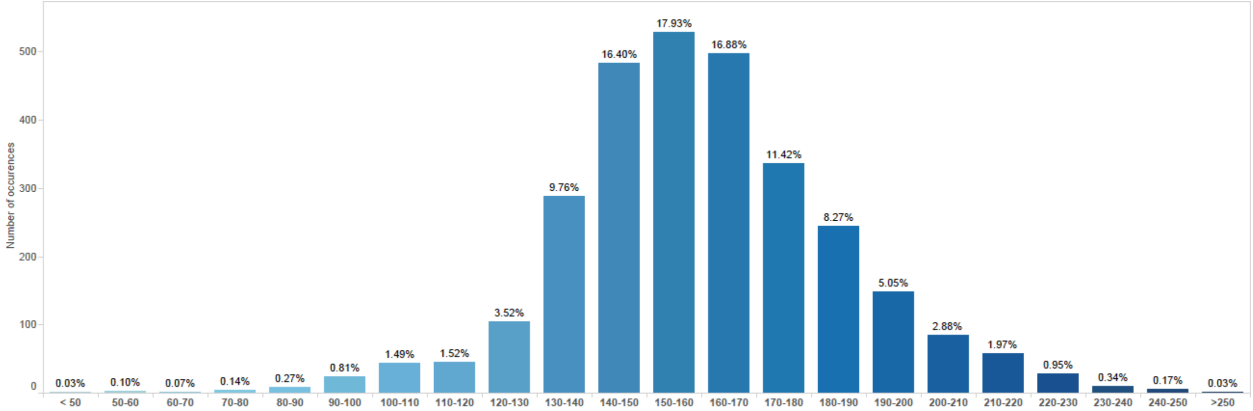


Figure 46*TC6 Madrid airport* **-** *Distribution of the score of facial images stored on chips*

Performance prediction is being obtained from the vendor to complete the feasibility analysis from a quality point of view for the Final Report.

4.3.3 Duration

The points of measurement for the duration of the e-MRTD facial image capture are:

	Measured from …	***To …***
Measurement 1	The first attempt at performing passive authentication	The successful passive authentication
Measurement 2	The first attempt at reading DG2	The successful capture of the facial image in DG2
Measurement 3 (= Measurement 1 + Measurement 2, with some possible overlap)	The first attempt at performing passive authentication	The successful capture of the facial image in DG2

Measurement 1: Duration of passive authentication

The graph below presents the time needed to perform passive authentication.

It can be seen that, in 97% of the cases, passive authentication took less than 4 seconds. Cases where passive authentication took longer than 8 seconds were extremely rare (0.07% of the cases).

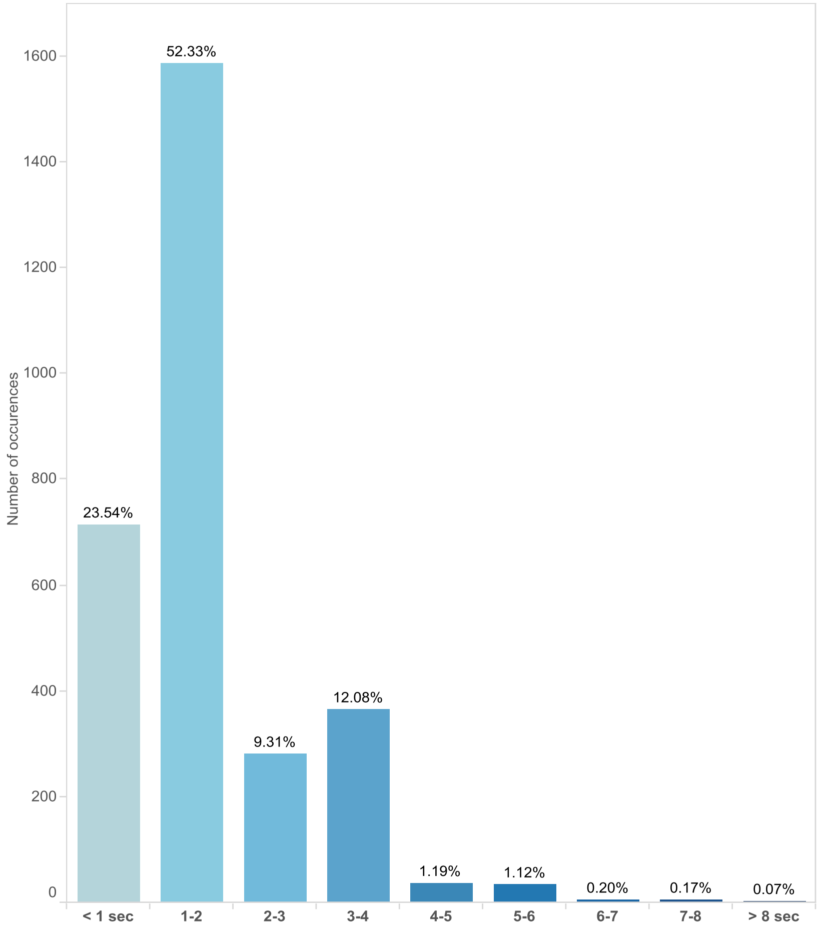


Figure 47 *TC6 Madrid airport - Distribution of passive authentication duration*

In addition, it can be seen from the graph below that there was a discrepancy in the duration of passive authentication based on the country issuing the passport. For example, performing passive authentication on Argentinian Passports required less than half the time than on US passports.

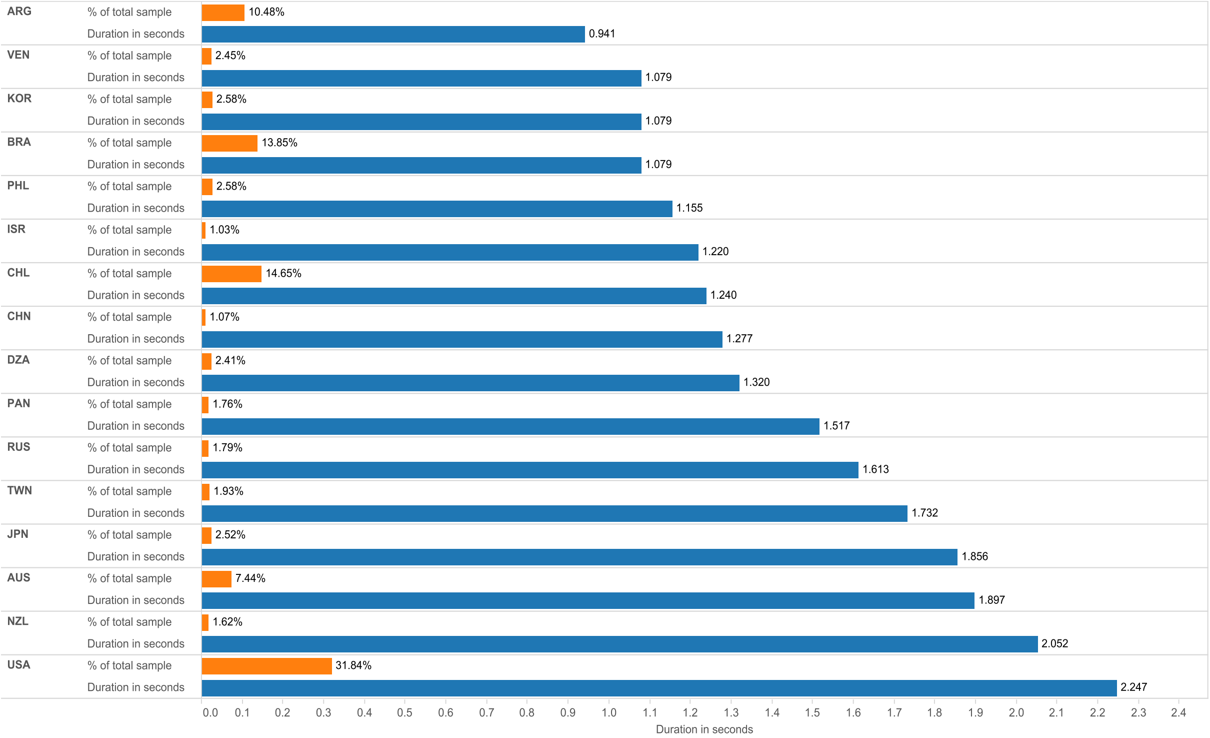


***Figure 48** TC6 Madrid airport - Breakdown of the average duration of performing passive authentication based on the issuing country (in blue) and the proportion of these passports in the sample (in orange)*

Measurement 2: Duration of DG2 reading

The graph below presents the time needed to capture the facial image from the passport (DG2 reading).

It can be seen that, in 94% of the cases, the reading of DG2 took less than 5 seconds. Cases where reading of the facial image (DG2) took longer than 6 seconds were rare (3% of the cases).

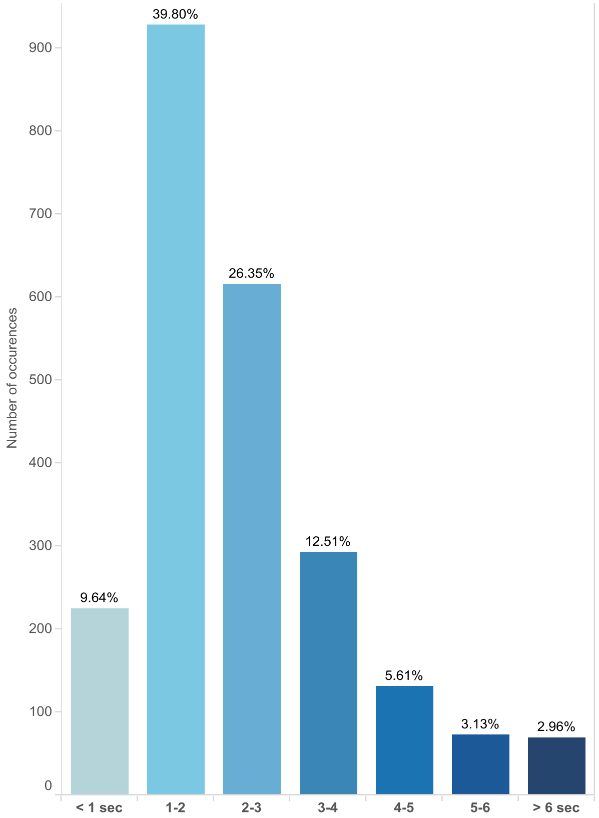


Figure 49 *TC6 Madrid airport - Distribution of DG2 reading duration*

Measurement 3: Duration of PA and DG2 reading

The graph below presents the time needed to capture the facial image (DG2 reading) and perform the Passive Authentication from the passport.

It can be seen that, in 85% of the cases, the reading of DG2 and Passive Authentication took less than 6 seconds. Cases where these two processes took longer than 10 seconds were rare (2% of the cases).

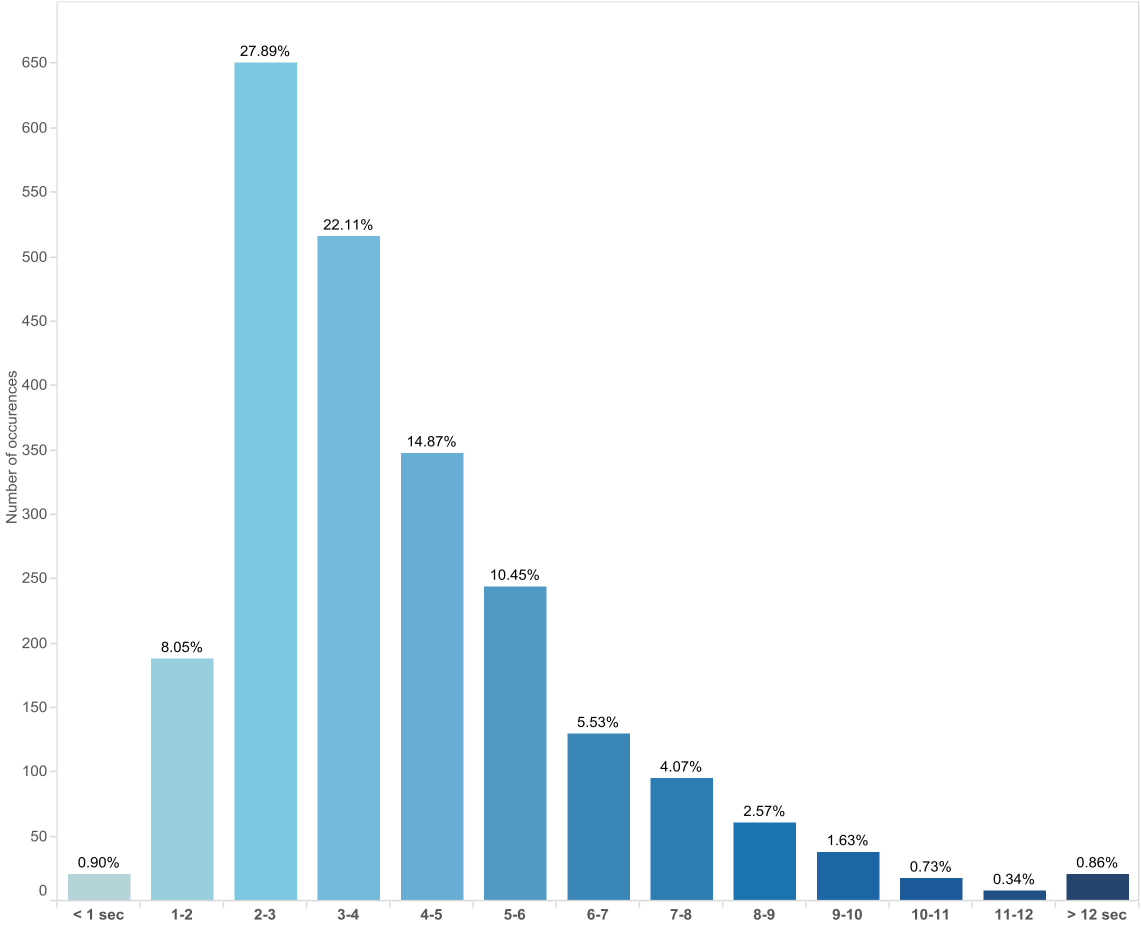


Figure 50 *TC6 Madrid airport - Distribution of PA and DG2 reading duration*

4.3.4 Security: added complexity of passive authentication

Reading the FI from the e-MRTD chip requires at least passive authentication to be performed.
Passive authentication (PA) consists of verifying the signature of the Document Signer over the Document Security Object. This relies on a two-layer certificate chain, enabling an inspection system to verify the authenticity and integrity of the data stored on the e-MRTD's chip.[30]

[30] The main components are:

- The root CA in the scheme is the Country Signing CA (CSCA), which authorizes Document Signers (DS) to sign the Document Security Object (SOD) on the chip. The CSCA certificate is distributed bilaterally by diplomatic exchange to relying States or obtained through masterlists which themselves are signed using issuer private keys that can be used to ensure their validity;
- The DS certificate may be obtained through diplomatic exchange with the issuing entity, obtained from the ICAO Public Key Directory (PKD) in some cases or otherwise obtained from the chip of the eMRTD where it is

The execution of the PA is a functionality that is part of the overall functionality of an IS. For this, the required certificates need to be in place, and the CRL needs to be checked for certificate revocation.

The cryptographic operations are well-known and have been standardised for many years by ISO and PKIX. However, the global set-up required to achieve trust amongst a community as diverse as the ICAO members and non-membersis a challenge due to its complexity.

4.3.5 Desk research

The basic aspects of reading the chip are addressed in the section on reading the facial image from the chip. Furthermore, foundation reading material with regard to cryptography was reviewed. This material is listed in section 10.4.5.

Minimal actions that need to be undertaken for managing certificates include:

- Key generation needs to be controlled;
- A certificate creation procedure needs to be put in place between the DS and the CSCA;
- The CSCA and DSCA need to make up-to-date revocation information available (CRL or OCSP31);
- Exchange (bilateral or central approach) of certificates;
- Validation of received certificates by relying party;
- Distribution of certificates and CRL/OCSP information to the Inspection System;
- Use of the appropriate certificates and up-to-date revocation information in the IS when performing the PA.

From desk research it became apparent that PA should not add 'additional complexity' since its usage is mandated by the SBC and MS should already have implemented the relevant procedures. However, it appears that PA is not performed consistently.

According to the 2014 [PRESSURV] survey, some countries do not electronically read ePassports, which is a prerequisite to performing PA.

4.3.6 Findings

4.3.6.1 Operational information

The information presented in this section was provided by Frontex, the Dutch department of Justice and Germany.

The three most common known issues related to PA reported by these organizations are:

- The use of expired certificates to sign the document;
- Errors in the encoding of the various data elements of the e-MRTDs Logical Data Structure (LDS);
- New type of passport reaching their borders before the certificate does.

often stored. If obtained from the document, best practices suggest it should be cross-checked against an external list of DS certificates or using the root CSCA certificate;

- Furthermore, Certificate Revocation Lists (CRLs) are published on the PKD and exchanged bilaterally.

[31] On-line Certificate Status Protocol (OCSP), the de facto mechanism in today's PKI to provide revocation information in an interactive way, as opposed to the original but non-interactive approach to use CRLs.

The third issue happens even with European passports. The Dutch department of Justice observed that only 4 countries are uploading regularly the certificates in the ICAO PKI (out of the around forty who formally joined).

4.3.6.2 Partial use of ePassport chips

Some Member States are not reading the ePassports' chips, which is a prerequisite to performing PA. Details with regard to the use of electronic reading equipment can be found in [PRESSURV].

Possible solution: equip IS with e-reading capability including PA performance.

4.3.6.3 Non-harmonised work processes and procedures

Currently there is a lack of mature procedures and harmonisation in work processes between different MS and other stakeholders.

Possible solutions: The minimal operating condition of an IS could be formalised and a conformity assessment thereof could be defined. Inspection Systems could then be subjected to such operational conformity assessment before being put into operation.

4.3.6.4 Missing cryptographic prerequisites

In some cases, performing PA results in an authentication failure because the required cryptographic prerequisites are not in place (certificates, CRL check).

Possible solutions: Systematic publication of certificates through e.g.:

- Master List approach (e.g. German Master List, Schengen Master List)
- Centralised control of certificate validation and management

This could be combined with the aforementioned conformity assessment of the operating conditions of an IS before being put into operation.

4.4 TC4 Technical and operational questions

4.4.1 Success/failure rate

Two main success conditions have been observed on the field when it comes to capturing the live facial image:

Success condition 1: Matching between e-MRTD facial image and live facial image could be performed within a certain timeframe.

Success condition 2: Quality threshold for the image reached within a certain timeframe.

The graph below presents the success rate of live facial image enrolment.

The success condition applied in Madrid is Success condition 1: Matching could be performed within a certain timeframe, the timeframe being 30 seconds and the threshold value 30 on a scale of 100 (which represents a FAR of approximately 0.3%).

It can be observed that the enrolment was possible in the absolute majority of cases (96%).

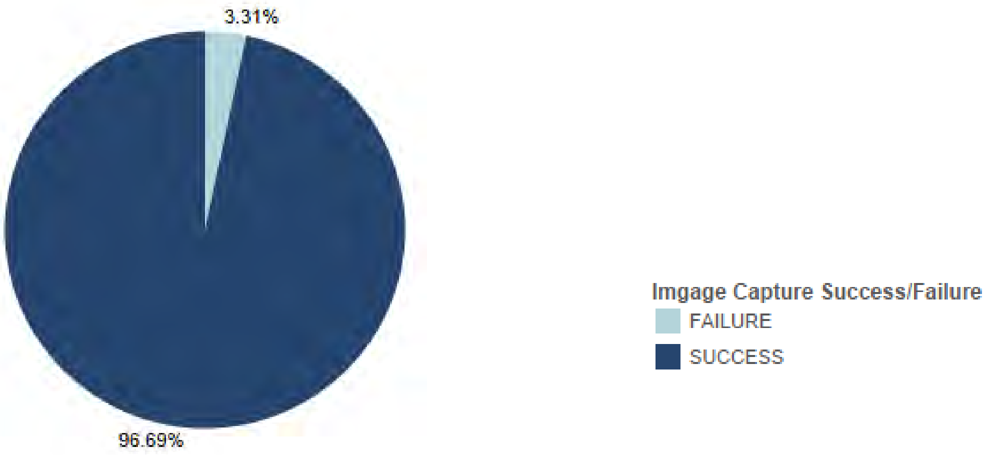


***Figure 51** TC4 Madrid airport - Success/failure ratio for live facial image enrolment*

4.4.2 Quality

Live facial image is evaluated based on one of two criteria, or both, depending on the data received from the MS:

- ICAO Document 9303 guidelines (extract);
- Vendor quality index

The indicator retained for Madrid Airport is the vendor's quality index.

The graph below presents the quality score results of the live facial image obtained in Madrid. The score is based on the vendor's quality index.

As the graph shows, the majority (over 87%) of live facial images present a quality above 80 , which has been seen to allow matching with another facial image of similar quality. Comparison with the facial image on the chip is presented in the summary, section 4.6.2.

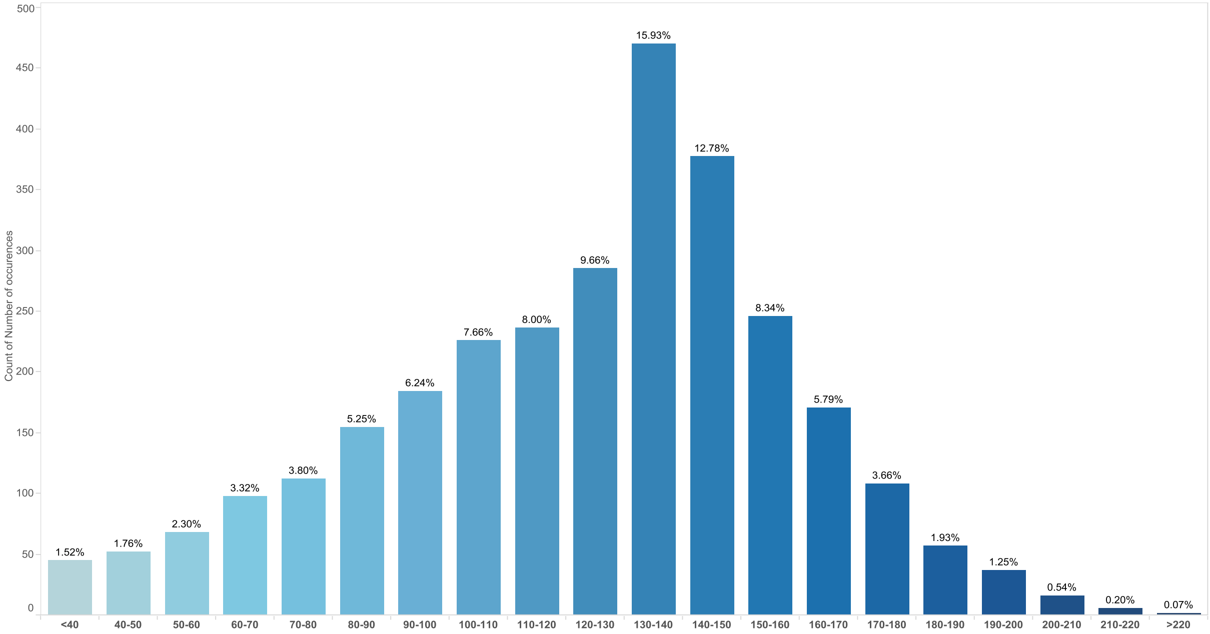


***Figure 52** TC4 Madrid airport - Distribution of live facial image score*

Performance prediction is being obtained from the vendor to complete the feasibility analysis from a quality point of view for the Final Report.

4.4.3 Duration

The points of measurement for the duration of the live facial image enrolment are:

Measured from …	***To …***
The first shot attempt	1. The successful capture; or
	2. Camera system timeout

The graph below presents the time needed to enrol the live facial image.

It can be observed that, in 85% of cases, the facial image could be captured very fast (in less than 4 seconds).

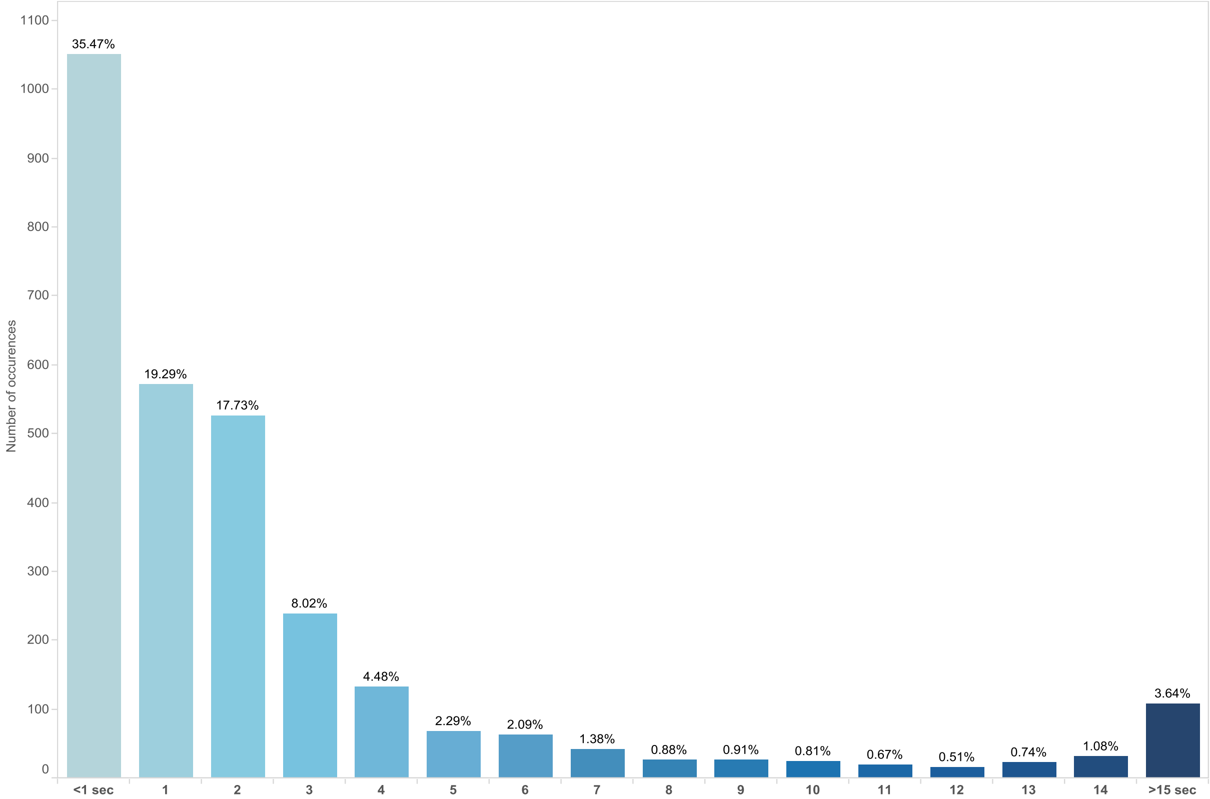


Figure 53 *TC4 Madrid airport - Distribution of enrolment of live facial image duration*

4.5 TC7 Technical and operational questions

The purpose of the tests was to attempt image matching between the chip's facial image captured in the scope of TC6 and the live facial image captured in scope of TC4, in order to perform local automated bearer verification at the border based on the facial image biometric identifier.

4.5.1 Success/failure rate

The graph below presents the success rate of matching between the chip's facial image and a live facial image.

The success condition applied in Madrid is: matching score is at least 30 on a scale of 100. This score is used throughout Madrid airport on other projects dealing with biometric recognition, and corresponds to a False Acceptance Rate (FAR) of approximately 0.3%.

It can be observed that the matching was possible in the majority of cases (80%) and that, in some instances (20%), a successful matching could not be done between the live facial image and the e-MRTD facial image. Further analysis will be performed to understand the origin of these failures (e.g. FRR, equipment problem).

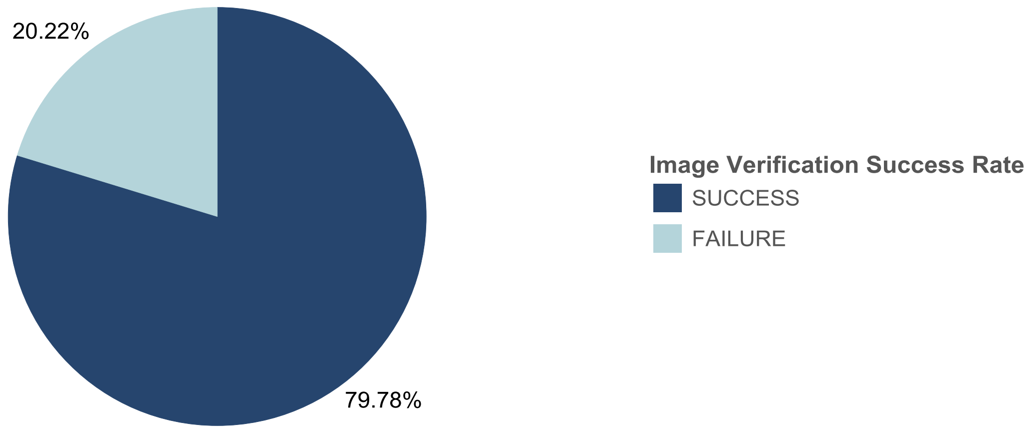


Figure 54 *TC7 Madrid airport - Success/failure ratio for matching between the chip's facial image and a live facial image*

4.5.2 Duration

The point of measurement for the duration of the facial image matching is:

Measured from …	***To …***
The first attempt at performing matching	Successful matching (above threshold)

The starting point to consider for the matching attempt should be considered carefully. For example, in cases where a video is taken, the attempt to perform the live capture can start early while trying to perform the matching at the same time.

The solution deployed at Madrid Airport did not make it possible to record duration values for facial image matching.

4.6 TC6, 4 and 7 Technical and operational questions

4.6.1 Success/failure rate

Success condition: Capture of the two images and matching could be performed within a certain timeframe.

From the graph below it can be seen that approximately one third of participating TCNs didn't manage to get their live facial image matched with the facial image stored in the chip. It can be seen that the highest comparative point of failure is the Passive Authentication.

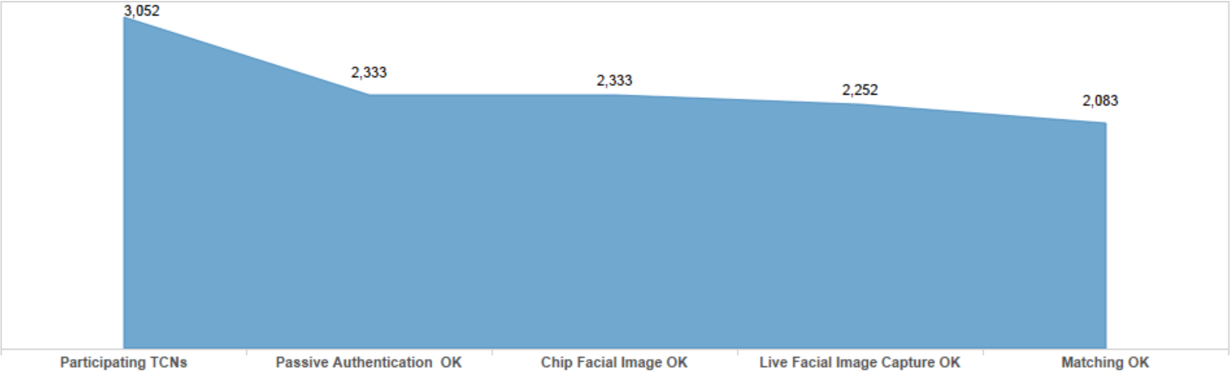


Figure 55 *TC4, 6 and 7 Madrid airport - Success rate at each step of the process*

4.6.2 Quality

In this section, we examine the results of facial-image focussed test cases together in order to examine general questions regarding the use of the facial image as a biometric identifier.

When comparing the quality scores of facial images stored on chips and live facial images at Madrid Airport, it is apparent that better quality can be achieved from facial images on chips. Indeed, only around 8% facial images on chips have a quality score below 120, compared to 39% for facial images captured live.

The higher quality can partly be explained by the more controlled environment in which pictures used for passports issuance are taken, compared to the variable and less optimal environment at the border.

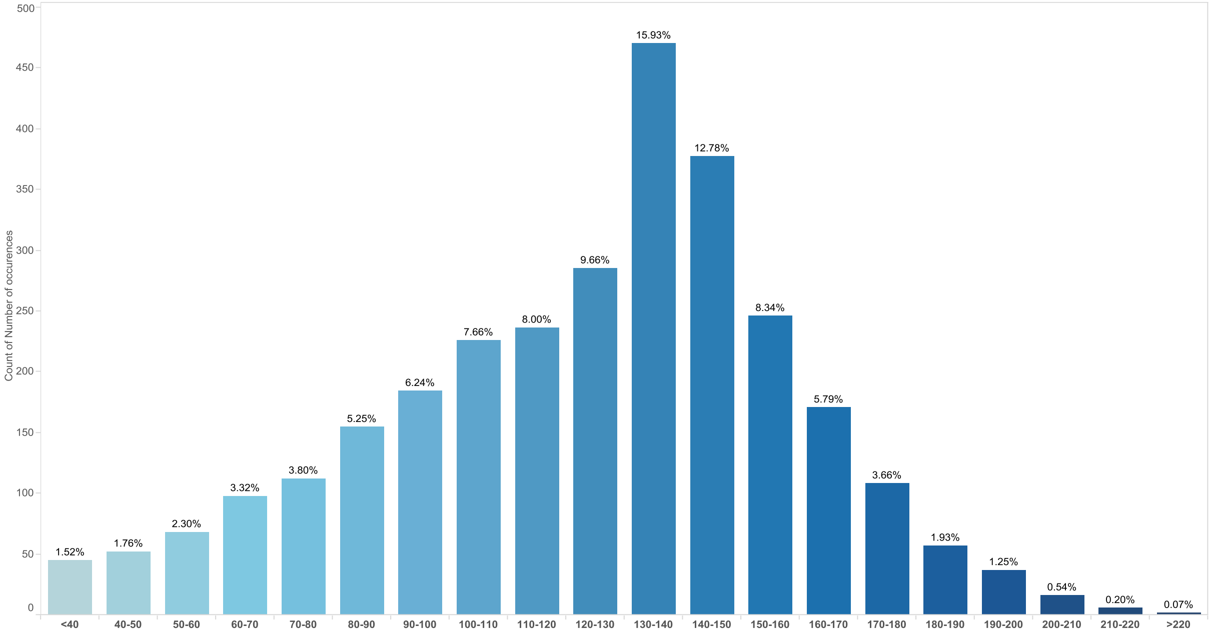


Figure 56 *TC4, 6 and 7 Madrid airport - Distribution of the score of live facial image*

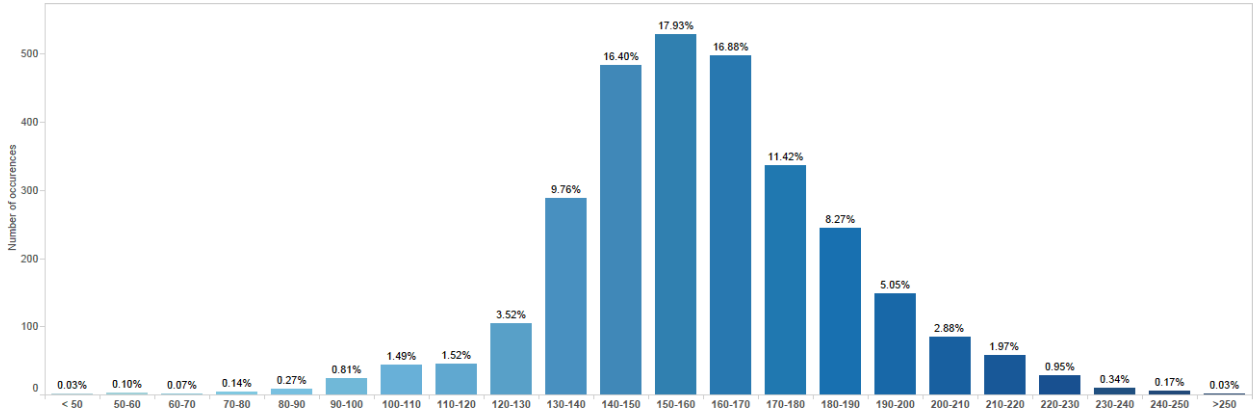


Figure 57 *TC4, 6 and 7 Madrid airport - Distribution of the score of facial images stored on chips*

Performance prediction is being obtained from the vendor to complete the feasibility analysis from a quality point of view for the Final Report.

4.6.3 Duration

The point of measurement for the duration of the facial image tests (TC4, 6 and 7) is:

Measured from …	***To …***
The first attempt at performing matching	Successful matching (above threshold)

Potential ways to accelerate this process are looked into in section 4.6.4. Potential accelerator: Enrolling the live facial image at the same time as capturing the facial image from the chip.

The graph below shows that when the attempt was successful, the steps involving facial image capture (live and from the chip) and facial image matching represent a small fraction of the border control total time (approximately 10%).

In this case, the Matching Time is 0: it is being recorded as part of the live image capture time as the two actions take place simultaneously.

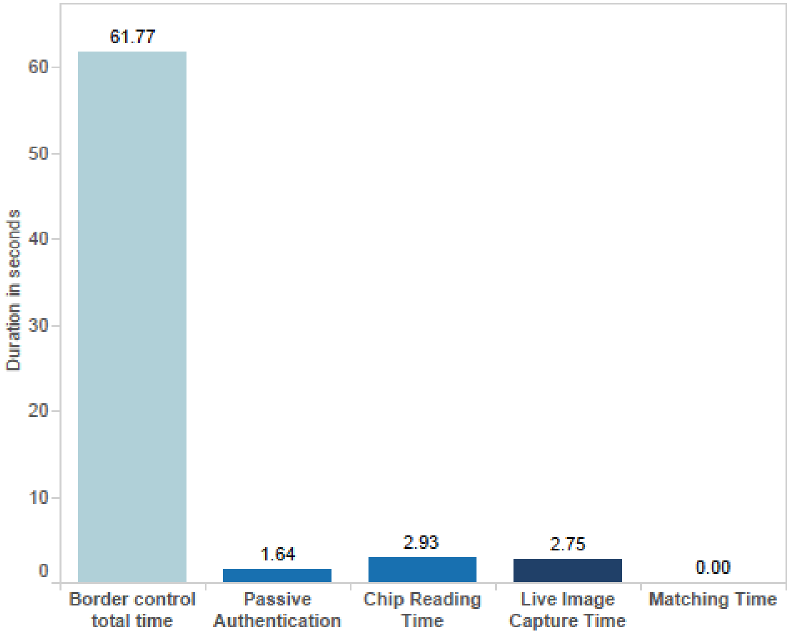


Figure 58 *TC4, 6 and 7 Madrid airport - Average duration per step of the combined process*

Unsuccessful attempts on the other hand, depend on the timeout setup at the BCP. At Madrid Airport the timeout was setup at 40 seconds. However, it was observed that the absolute majority of cases were either successful after around 10 seconds, or turned out to be successful.

4.6.4 A potential accelerator: Enrolling the live facial image at the same time as capturing the facial image from the chip

Both activities take place at the Border Control Point when a border check is performed:

- Reading the chip to obtain the facial image (and other relevant information) is described in the section that addresses reading the facial image from the chip;
- Enrolment of a live image of the traveller is a completely separate procedure that is, at first sight, completely unrelated to the chip reading.

It has been agreed that the question should not be interpreted too literally: "at the same time" is not necessarily simultaneously.

The extent to which chip reading and image taking influence each other, and can potentially be parallelised is a question of workflow organisation, of technology, and of environmental conditions (and the control thereof).

Elements considered to be within the scope are:

1. e-MRTD containing chip with embedded FI
2. IS consisting of reader, application platform, application
3. Camera
4. Photo booth or similar location
5. Operator, typically a Border Guard
6. Traveller
7. Operational conditions that are representative for a BCP

However, the main focus consists of the e-MRTD and the IS.

4.6.5 Desk research

ICAO 9303 Part 1 Volume 2 Specifications for electronically enabled passports with biometric identification capability. This ICAO document points to ISO 19794, which is a multi-document standard, of which **ISO 19794-5 'Face image data'** is the application to facial image recognition. This standard is applicable to both manual and automated recognition. It includes 'best practices' for images. Detailed requirements on the image are specified in ISO/IEC 19794-5 which provides a Face Image Format for face recognition applications requiring exchange of face image data.

Furthermore:

- Reading the chip is addressed in the section that covers reading the facial image from the chip (see above);
- Live image taking is specified by Frontex in [FTXBPGABCT].

4.6.6 Observations

4.6.6.1 Operational observations

The following operational observations were made.

Workflow aspects

- Traveller cannot simultaneously look at the reader to position his e-MRTD and at the camera;
- In the case of ABC gates, there is a high variation of workflow between different countries;
- There should be no parallelisation, as then the traveller does not know what is expected of him, and he doesn't learn the process quickly32.

Technological aspects

Finland has put forward that, technologically, it is feasible to capture the 2 facial images at the same time.

Germany has put forward that video capture might be good for identification but not necessarily for enrolment, and that what is required is auto-capture of high quality images, parallel to live facial image assessment.

4.6.6.2 Conditions

Conditions under which the FI can be read from the chip while the live facial image is being taken are specified below from a workflow, technology and environmental standpoint.

Workflow conditions

The two operations are essentially unrelated but to perform them at the same time, two options can be considered:

- Full attention of the traveller and the border guard is required;
- Install video camera that automatically captures FI while the traveller is performing another step of the process;
  - Ideally the video camera should meet the gaze of the traveller;

[32] Suggestions made at the expert meeting held in Madrid in April 2015. Yet, these are observations from the field and eu-LISA does not have quantified evidence so far.

- Some ABC gates and kiosks already have a workflow allowing this.

Regardless of the option chosen, mobile equipment remains challenging (requires the Border Guard to "aim" for the traveller's face).

Technology conditions

To enable the two operations to be performed at the same time, the video camera should have:

- Continuous image capture;
- Autofocus or light field camera;
- Adjustable capture height.

The system should be able to handle several processes simultaneously.

Environmental conditions

Challenging environments (e.g. at night, inside a car)

Garments worn in certain environmental conditions (e.g. hat, scarf, sunglasses)

4.7 Users' feedback

4.7.1 Border guard's survey

14 border guards participated and replied to the survey from Madrid airport.

They have been asked to provide replies after the first work package (with new equipment: camera and FP reader with slap technology) and after the second work package (with existing equipment, *i.e.* fingerprint reader).

The **total number of replies is thus of 27 since 1 border guard replied only once to the questionnaire regarding wave 1 (existing)**.

The following dashboard presents a summary of replies[33].

Overall feedback[34] ★ ★ ★

Border Guard		Traveller
100% felt more confident with equipment regardless of whether the equipment was new or existing	100% rate the usability of equipment as good regardless of whether the equipment was new or existing	86% of replies indicated good acceptance of travellers regardless of the equipment, with the disclaimer that longer queuing time was not well always received[35]

Potential improvement points

[33] Percentages are calculated per question and are based on the number of replies given. In some cases, BGs have given more than one reply to one question.

[34] Rating : 3 * = good / 2* = neutral / 1* =weak

[35] This is aligned with score of travellers' survey: 94.4% are satisfied or very satisfied.

Border Guard		Traveller
In 15% of replies, border guards indicated that integrated and automated cameras could improve the process and equipment[36]	**New equipment**: in 29% of the replies, the equipment could be more ergonomic **Existing equipment**: in 85 % of cases, the equipment could be more ergonomic	**New equipment**: in 79% of replies, more guidance would be needed for travellers **Existing equipment**: 15% think that more guidance to travellers would be needed

Potential show-stoppers

Traveller	
Language 5%	Hardware problem 60% (applicable to both new and existing equipment)
Longer queuing time has been identified as an issue for some travellers	Signal-system problem 35% (applicable to both new and existing equipment)
	-

Observations and preliminary conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- **The aim of the Pilot** was welcomed:
  - Most travellers value the increase of security provided;
  - They liked the idea of smart borders without border guards.
- **Human factor** and **communication** are paramount:
  - Passengers felt more confident with border guards explanations (e.g. process is facilitated when border guards indicate which fingerprints must be given);
  - Difficulty to communicate with some TCNs (language barrier) caused abortion of tests in some cases.
- **Equipment is not 100% reliable and stable**
  - Some problems with the camera have been experienced: luminosity and brightness have a consequent impact on facial recognition (as explained in section 4.8);
  - FP reader is sometimes unstable for both new and existing equipment;
  - Equipment should indicate whether successful capture of FP has been success would be useful in order to better guide passengers and avoid mistakes;
  - Passport origin can impact loading time as explained in section 4.8.

[36] The camera was not integrated.

4.7.2 Travellers' feedback

The results collected in Madrid and summarised in the chart below show that travellers responded overwhelmingly positively. Less than two percent of travellers were dissatisfied.

It should be noted that the tests were run in parallel with TC1, using both new and existing equipment. The results shown belov :est conditions were more difficult for tra

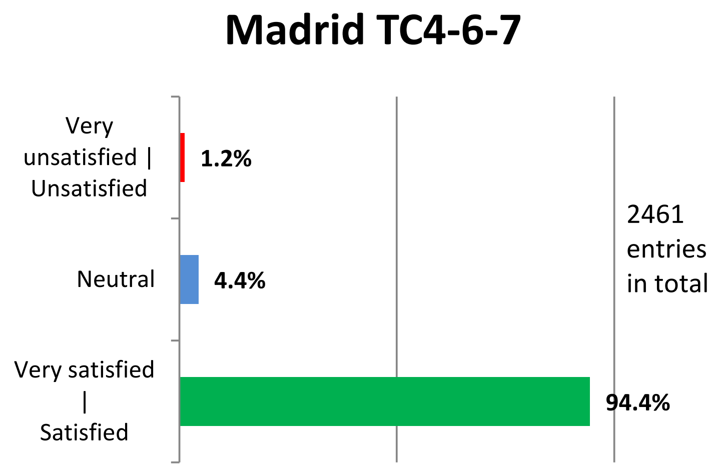


Figure 59 *TC4, 6 and 7 Madrid airport - Traveller satisfaction survey results*

4.8 Constraints

4.8.1 Environmental conditions

The tests took place at Madrid airport, with indoor conditions.

Some Border Guards suggested that light coming from a glass wall behind the booths caused some difficulty. Otherwise, no environmental conditions were noted as having negatively influenced the proper capture and verification of live facial images.

4.8.2 e-MRTD facial image reading influencing factors

States issuing e-MRTDs include a facial image of the document owner according to ICAO specifications [ICAO9303P1V2]. The facial image is stored as a JPEG/JPEG2000 encoded face in DG2, and the display portrait is stored in DG5.

CSCA – The Country level

In order to protect the chip's contents, including the facial image, Issuing States establish a Country Signing Certification Authority (CSCA).

The CSCA certificate as well as corresponding revocation information can be made available either through bilateral exchange or through the use of Master Lists.

The CSCA signs the certificate(s) of its Issuing Authority's Document Signing Certification Authority (DSCA).

DSCA – The Document Signer level

The Issuing State's DSCA will sign the e-MRTD's Document Security Object ('SOD') which contains the hashes of the document's Logical Data Structure (LDS). Upon arrival at a Border Control Point in a Relying State, the Inspection System will read both the optical and electronic information stored in the e-MRTD. The execution of the Passive Authentication includes recalculation of the hashes, the validation of the certificate chain and the verification of the signature of the SOD.

The main stakeholders and components involved in reading the facial image from the chip are illustrated in the figure below.

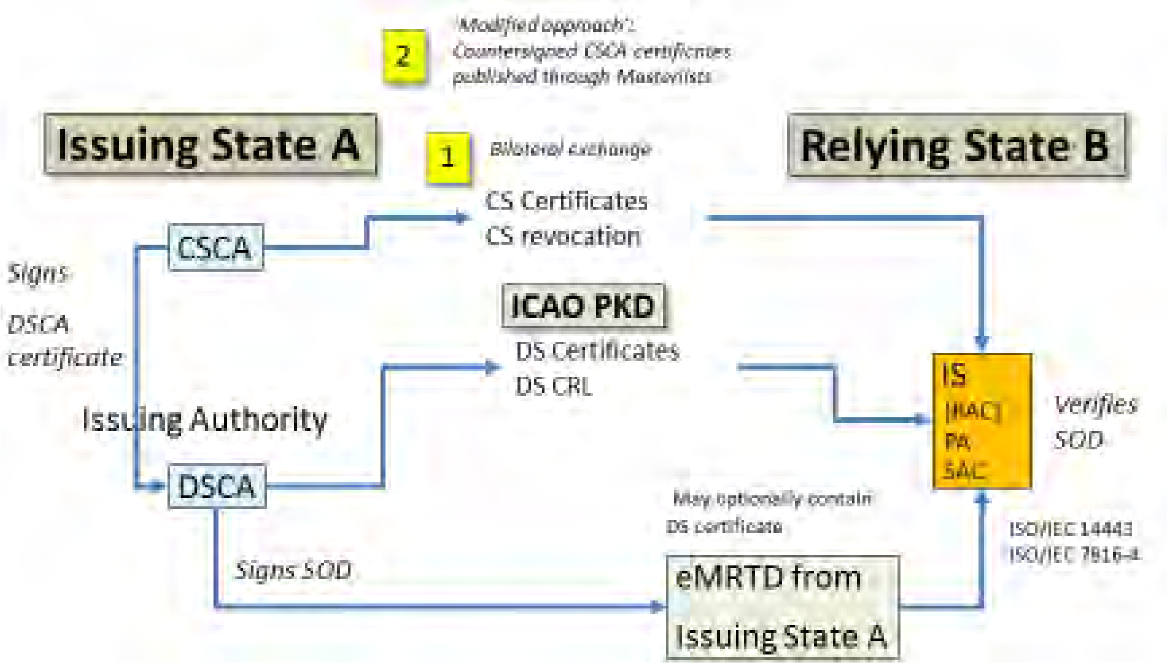


Figure 60 *Overview of FI-chip reading*

4.8.3 Desk research performed

A range of secondary sources were used for desk researching this question. They are listed in section *10.4.4* References with regard to reading the FI from the chip*.*

The steps involved in e-MRTD authentication (including the verification of the authenticity of the FI data) are described in [FTXBPGABCT], section 4.5.

The steps in reading an FI from a chip embedded in an e-MRTD are described in section 10.4.2

The e-MRTD chip data structure is described in section 10.4.1

4.8.4 Passive Authentication procedure

Passive Authentication uses a digital signature to authenticate data stored in the data groups on the MRTD chip. This signature is generated by a Document Signer (e.g. the MRTD producer) in the personalization phase of the MRTD chip over a Document Security Object containing the hash values of all data groups stored on the chip. For details on the Document Security Object, Document Signers, and Country Signing CAs the reader is referred to [2].

To verify data stored on an MRTD chip using Passive Authentication the terminal has to perform the following steps:

1. Read the Document Security Object from the MRTD chip.

2. Retrieve the corresponding Document Signer Certificate, the trusted Country Signing CA Certificate, and the corresponding Certificate Revocation List.

3. Verify the Document Signer Certificate and the signature of the Document Security Object.

4. Compute hash values of read data groups and compare them to the hash values in the Document Security Object.

Passive Authentication enables a terminal to detect manipulated data groups, but it does not prevent cloning of MRTD chips, *i.e.* copying the complete data stored on one MRTD chip to another MRTD chip.

Source: BSI, Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token

4.8.5 Chip reading procedure

The following possible reasons for failing to read the FI from the chip were identified from desk research:

- If chip and/or reader do not comply with the required ISO standards, the initialisation will fail. Subsequently reading the FI from the chip will not be possible. The same holds true if the chip, the antenna or the link between chip and antenna are defect. These specifications were later refined in [ICAO9303P3V2], and complemented by the ICAO Doc 9303 Supplement [ICAO9303SUP];
- If multiple chips respond and the anti-collision fails, it will not be possible to initialise communication with the chip (and subsequently read the FI from the chip);
- For the IS to verify this integrity, the Document Signer's Public Key is required. This key should be obtained in a certificate from the PKD and stored in the IS. If this is provided on the chip, the certificate may also be read from there. The IS should verify the certificate containing the DS Public Key using the Issuing State's Country Signing CA Public Key from a corresponding certificate. The verification of the integrity of the Elementary Files (EF), which constitute the individual files within the chip file system, will fail if either or both of these certificates are not available, or are revoked;
- Both OCR and keyboard entry may fail. For those e-MRTDs that implement BAC, the reading will then fail;
- For e-MRTDs that implement Active Authentication37 (AA), failure of AA execution may be taken into consideration by the IS when processing information from the e-MRTD such as FI. This may lead to unavailability/rejection of the FI.

4.8.6 Findings

The following conditions were found to influence the possibility of reading the facial image from the e-MRTD: Each of them will be further detailed, and possible solutions to address them are proposed.

4.8.6.1 Operational observations

General operational information collected

MSs seem not to have gathered information about this matter in the past, and about FI reading in particular. This could be an aspect to further investigate with the collaboration of the MSs (which is outside of the scope of this document).

There are well-known exceptions such as the Malaysian passport (seems not to follow ICAO rules) and the Nigerian passport, which lacks BAC.

[37] Active Authentication is available on eMRTDs that have their individual cryptographic key pair per chip. The public key will be made available in a certificate. AA involves using the chip's private key to transform an IS generated challenge into a response which can be verified by the matching and certified public key.

4.8.6.2 Damaged chip/antenna

This condition is encountered when either or both of these observations can be made:

- The embedded chip is defective and unresponsive to power-up (e.g. after application of overvoltage);
- The embedded antenna is defective;
- The link between the two (chip/antenna) is severed, so the chip is cut off from communication.

Possible solutions:

In this case, travellers could be invited to pre-check their e-MRTD, e.g.

- Via a test application using readers e.g. at municipalities, or;
- Via an app on RFID/NFC smartphones or tablets.

4.8.6.3 Non-ICAO-compliant passport

This condition includes:

- It has been observed that in some cases non-ICAO compliant passports have been issued by e.g. Brazil, Malaysia, China, and Russia;
- DG2 encoding issues (JPEG);
- Inconsistency between visual and electronic Machine Readable Zone (MRZ) leading to rejection of the e-MRTD;
- Use of incorrect Object Identifier for the IdsSecurityObject, leading to PA failure (as per [FTXOTEP], section 2.5.6.1);
- Lack of conformity in implementation of security safeguards (as per [FTXOTEP], section 4.3.2).

Possible solutions

In this case, the following options could be considered:

- Conformity assessment by either a central (e.g. European, ICAO) authority or a MS recognised CAB (Conformity Assessment Body);
- Use of defect list (similar to what is done by Germany) which is communicated between States;
- Use of and conformity assessment according to ISO Common Criteria protection profile such as:
  - BSI-CC-PP-0055 (BAC);
  - BSI-CC-PP-0056 (EAC);
  - BSI-CC-PP-0068-V2-2011 (SAC).

4.8.6.4 Lack of certificates (CSCA/DSCA) in the IS.

This also includes lack of access to up-to-date revocation information such as the required CRLs.

Possible solutions:

In this case, the following options could be considered:

- Follow regular PKI good practice (controlled key generation and certificate creation, distribution of root certificate with out of band confirmation, verification of entire certificate chain);
- Application of the ‘Modified approach’ with Master Lists38.

[38] cf. Meeting with COM on 13/05 on Schengen CSCA Master List

4.8.6.5 Non-conformant inspection systems.

It has been observed that a mandatory conformance testing is not defined or imposed. Frontex published various 'best practice guidance' documents. However, they are not a substitute for a conformity testing methodology, and an obligation/recommendation to apply it.

Possible solution: Definition of minimal mandatory conformance testing methodology. Evaluation of possibilities to enforce this and embedded self-check of the device.

4.8.6.6 Intentional and malicious chip disabling[39]

According to ICAO Doc 9303 part 1 volume 2 section IV paragraph 2.6 [3]: "Since e-passports with a non-functioning chip are still valid, disabling the chip may be a way to make falsification easier, not placing a chip makes counterfeit easier "

Possible solution: "When the chip is checked at first line border control and turns out to be broken, the passport should go to second line inspection".

4.8.6.7 Malicious chip replacement[40]

Possible solution:

- "Good implementation of the inspection system with all security mechanisms implemented";
- Encrypted chip ID in the ship and printed on the passport (QRcode) or embedded in the digital picture (steganography).

4.8.6.8 Broken cryptography

Possible solution:

Detective option: when the chip is checked at first line border control and the cryptography indicates a problem such as e.g. wrong signature, the passport should go to second line inspection.

Preventive option: conformity assessment as already described in the condition 'Using non-conformant inspection systems'.

4.9 Feasibility

[To be added in the Final Report]

[39] as per [FTXOTEP], section 2.5.4

[40] *Ibid.*

5. Iris

5.1 Introduction

[Treatment and cleaning of data to be finalised in the Final Report]

The Technical Study did not include an analysis of the impact of using iris as biometric identifier. Yet the Study states that the use of iris is a mature technology and there are examples around the world of using this as biometric identifier, also with large volumes of data. The Study recommends that the Pilot should include tests for enrolling the iris pattern of travellers.

5.1.1 Objective

One Test Case is considered for the iris biometric modality with the following objective:

1. **Enrol iris pattern (TC5) –** evaluate whether enrolling the iris is a valid complementary biometric identifier compared to facial image and fingerprints, for Registered Travellers.

5.1.2 Workflow of the test case

The process of testing TC5 is built upon a single step: capture iris pattern.

In some of the tests, this process will be combined with capturing a live facial image (*i.e.* in Cherbourg (FR) and in Iasi (RO)).

5.2 Methodology

The objective of the Test Case is addressed following the structure below.

1. **Operational and technological questions per type of BCP (land, moving train, air)**
   a. Success / failure: What is the success / failure ratio?
   b. Quality of the enrolment: What is the recorded quality?
   c. Duration: What is the process added duration? Can facial image be captured in the same step as enrolling the iris?
   d. Security: Is iris enrolment more or less prone to spoofing and which anti-spoofing measures need to be taken?
2. **Users' feedback**
   a. Perception of TCN's: What is the traveller's perception of the enrolment of iris?
   b. Feed-back from Border Guards: How do border guards experience the added step of enrolling the iris?
3. **Constraints:** Which environmental conditions do influence the quality and/or duration of the enrolment (e.g. ambient light)?
4. **Feasibility:** Can the iris be enrolled and verified at Land Borders, including when passengers remain in cars? If not what are the exceptions and why? This question will be answered on the basis of the findings of the questions above.

The iris Test Case has been mainly analysed through operational testing. Security aspects regarding iris spoofing vulnerability have been addressed by desk research in section d.

5.2.1 BCP selection

The iris Test Case will be carried out at the five following BCPs.

Air	**Land**	**Moving train**	**Sea (in cars)**
• Lisbon (PT)	• Sculeni (RO) • Kipoi (EL)	• Iasi (RO)	• Cherbourg (FR)

This interim report only gives an insight into the preliminary data gathered from Lisbon.

5.2.2 Type of equipment

5.2.2.1 Iris enrolment

Iris scanners can be described by three main characteristics.

Table 16 *Categories of devices for iris enrolment*

Mobile or fixed solution	**Fixed:** Requires a connection to a fixed element. **Mobile solution:** Can be freely transported and operated without space limitation.
Acquisition distance	**Acquisition distance <50 cm:** Potentially higher feeling of privacy intrusion. **Acquisition distance >50 cm:** Potentially lower feeling of privacy intrusion.
Facial Image capability[41]	**Yes, simultaneously**: Iris pattern and facial image can be taken at the same time. **Yes, not simultaneously:** Iris pattern and facial image and can be taken, but not at the same time or in the same conditions (e.g. the subject should be closer to the scanner for Iris capture). **No**: The Iris scanner cannot capture a facial image.

5.2.3 Configuration per BCP (Lisbon)

Table 17 *TC5 Lisbon airport – TC Configuration*

Duration of the test	3 weeks (from 13.04.2015 to 04.05.2015)
Timetable of the tests	08:00 to 15:00
Layout	Dedicated lane
Sample size achieved	2380
Technical integration	No
Integration within the regular border crossing process	No
Equipment type	• New fixed iris scanner, based on Video Capture technology • Acquisition distance: <50 cm • FI captured but not simultaneously with iris pattern
Enrolment/verification threshold	50 for Verification purposes, 76 for enrolment purposes. Scale of 100.
Travellers' survey	Self-service eu-LISA tablets on stands / Can be used by hosts if available
Test personnel	Shifts of 2 border guards

[41] More information on the usage of Facial Image as a biometric identifier, please refer to chapter 4

5.3 Operational and technical questions

5.3.1 Success/failure rate

The success condition is the successful capture of the iris pattern.

The graph below presents the success rate of iris pattern capture, as well as the conditions of success reached. At Lisbon Airport, two thresholds were defined: "Enrolment Quality" meant that the quality exceeded 76/100, and "Identification Quality" meant that the quality exceeded 50/100 but did not reach 76/100.

It can be observed that the capture was possible in the majority of cases (83%), and that in some occasions (17%), the iris pattern could not be enrolled at a good enough quality. Only a small proportion (5% for left iris and 3% for right iris) of total attempts was successful but did not reach the threshold for "Enrolment Quality".

At Lisbon airport, the device was setup to either succeed the capture of both iris patterns, or to consider it a failure. This explains the absence of difference between the success/failure ratios for left iris and right iris.

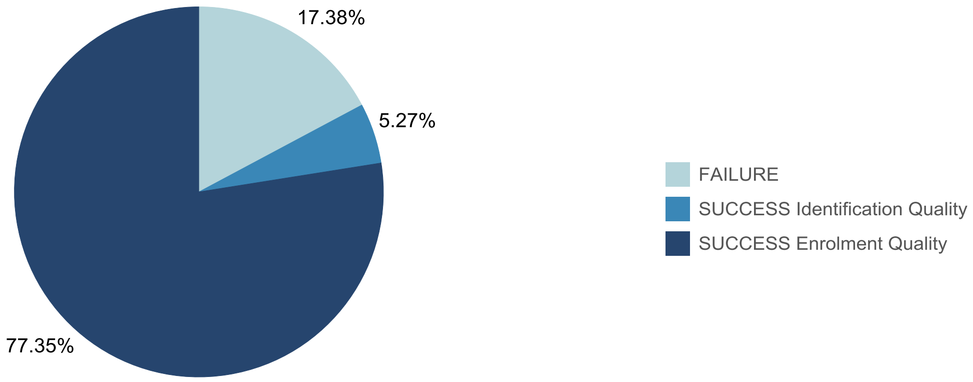


Figure 61 *TC5 Lisbon aiport - Success / failure ratio of left iris pattern enrolment*

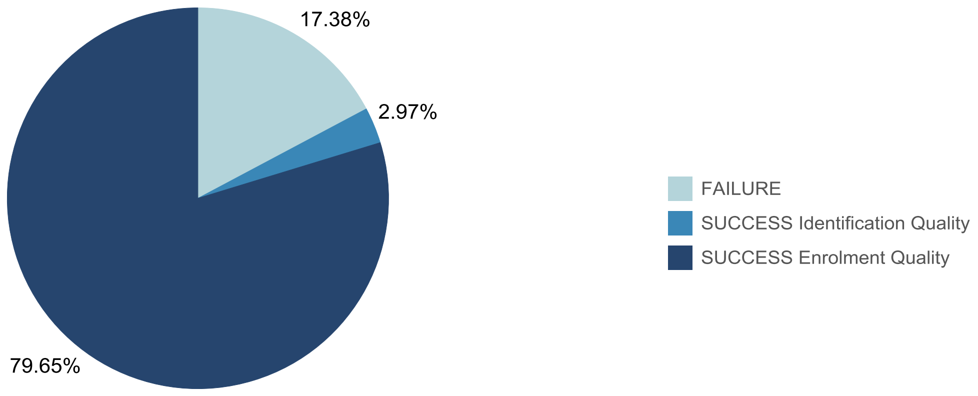


Figure 62 *TC5 Lisbon aiport - Success / failure ratio of right iris pattern enrolment*

5.3.2 Quality

The quality of the iris pattern captured live is evaluated based on one of two criteria depending on the data received from the MS:

- NISTIR 7820 (extract);
- Vendor quality index.

The indicator retained for Lisbon airport is the Vendor quality index.

The graph below presents the quality score results of the iris patterns obtained in Lisbon. The score is based on the vendor's quality index.

The setup at Lisbon Airport only recorded quality values for the successful enrolments. Out of these, it can be observed that the absolute majority (92% for left iris and 95% for right iris) of them were of quality superior to 80.

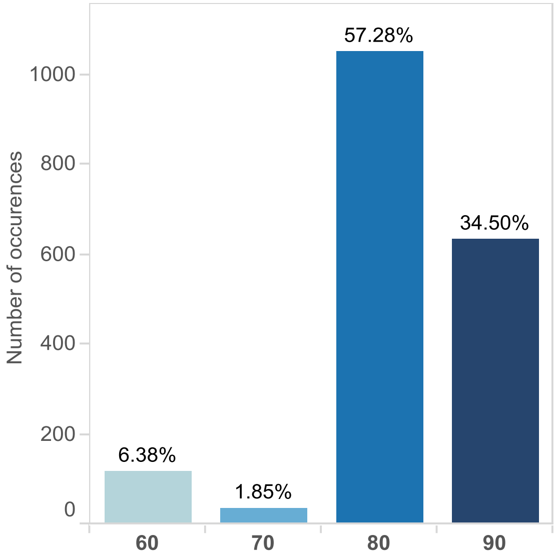


Figure 63 TC5 Lisbon airport - Distribution of the score of left iris patterns

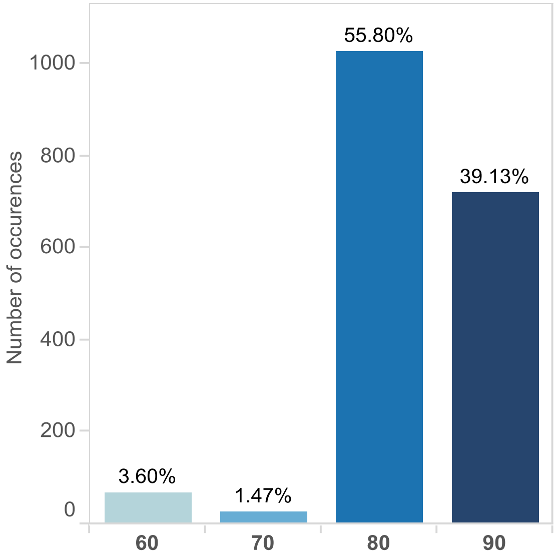


Figure 64 TC5 Lisbon airport - Distribution of the score of right iris patterns

Performance prediction is being obtained from the vendor to complete the feasibility analysis from a quality point of view for the Final Report.

5.3.3 Duration

The points of measurement for the duration of the eMRTD facial image capture are:

Measured from ...	**To ...**
The first attempt at capturing the pair of iris patterns	Successful capture

The graph below presents the time needed for capturing a pair of iris patterns.

It can be seen that in:

- 65% of cases, the successful enrolment of the pair of iris patterns was taking less than 12 seconds;
- 84% was taking less than 18 seconds;
- 95% was taking less than 30 seconds;
- 5% took more than 30 seconds.

The timeout was set at 40 seconds, and it can be seen here that raising the threshold higher than 24 seconds managed to capture only 10% of additional cases.

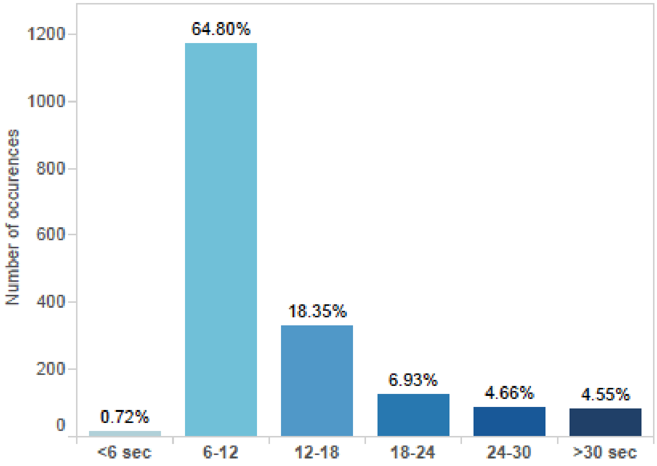


Figure 65 *TC5 Lisbon airport* ***-*** *Distribution of enrolment duration of a pair of iris patterns*

5.4 Security: Iris Spoofing vulnerability

Spoofing refers to using a fabricated biometric sample or physical trait to deceive the system into believing the sample is provided by a live and authentic user. With regard to counter-measures, liveness detection is a key factor. There are two major approaches with regard to liveness detection:

- Hardware-based systems – typically deploying additional sensors and software, may include measurements outside of the primary biometric mode;
- Software based systems - use image processing algorithms. As this is purely based on software, this approach is amenable to central deployment, which has benefits from a cost-effectiveness and convenience perspective.

With regard to reporting on spoofing, following terms are commonly used;

- Ferrfake – misclassified fake samples ('false acceptance');
- Ferrlive – misclassified live samples ('false rejection').

The methodology included:

- Using the results of competitions in which spoofing performance of different biometric modalities have been compared;
- Analysing state-of-the-art counter-spoofing measures and assess their described effectiveness;
- Seeking the opinions of experts at MS and international level.

Scope included:

1. Iris enrolment platform to establish base truth
2. Anti-spoofing safeguards
3. IS consisting of iris camera, application platform, application
4. Operator, typically a Border Guard
5. TCN traveller

5.4.1 Desk research

5.4.1.1 Introduction

A range of secondary sources were used to perform the desk research on this question. This included foundation reading material with regard to biometric recognition with a focus on iris technology from NIST, ISO, BSI, latest LivDet reports, as well as publications from Tabula Rasa and Fidelity.

Articles identified as particularly relevant to iris spoofing are listed in the appendix 10.5.3. Complete references are listed in the section 10.5.4. The main observations from these sources are described below.

Spoofing consists of a presentation attack at the sensor, indicated by arrow 1 on the figure below.

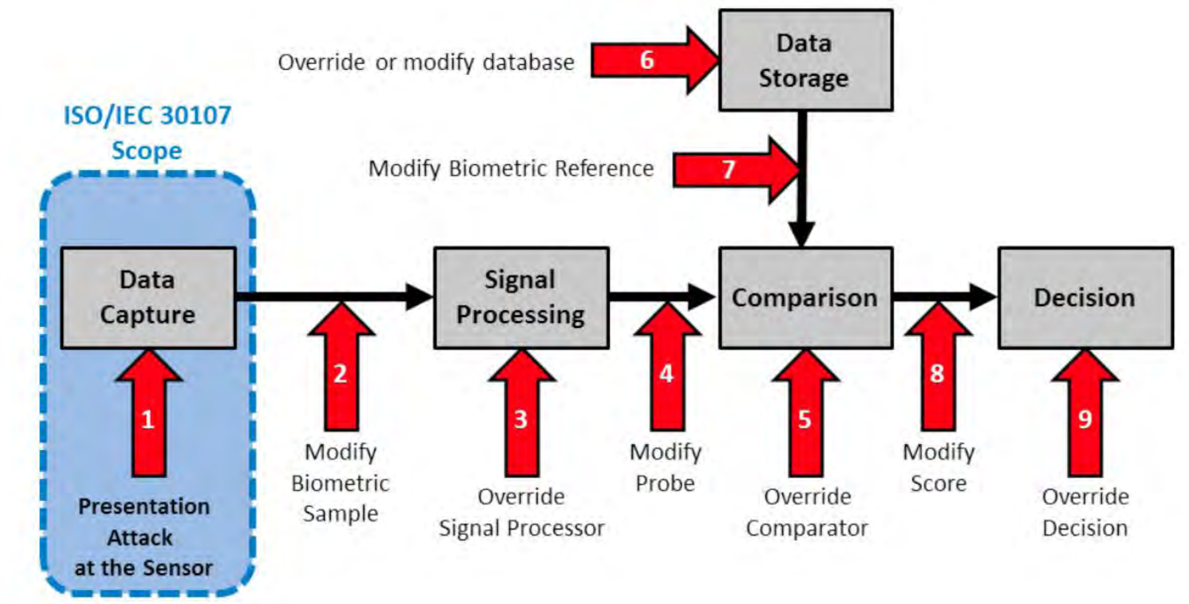


***Figure 66** Spoofing attack*[42]

It can be observed that 'Spoofing' corresponds to arrow 1.

Dr J. Daugman, the holder of the first patent for iris recognition that lead to widely deployed solutions, stated in his patent that the algorithms he proposed provide inherent liveness detection. The pupil diameter of a living eye undergoes small oscillations ("hippus") one or twice per second – thus can be used for liveness determination. This is also referred to in e.g. Bodade et al. 2009, 2011, and Huang et al. 2013.

Daugman's iris codes are 256 bytes. Due to radial correlations, there is a standard binomial distribution of 173 bits. Thus, the odds that two different irises might generate an identical iris code are 2 ^{173} or 10 ^{52}. Details are provided in the pristine source, US Patent 5.291.560.

Furthermore, multimodal can be considered as an anti-spoofing method but as it does not address iris spoofing as per the Pilot ToR question it is not addressed further.

5.4.1.2 ISO/IEC 30107

This standard aims to establish:

[42] *Source: Tabula Rasa D5.7: Standards for security evaluation under spoofing attacks*

- Terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods;
- A common data format for conveying the type of approach used and the assessment of presentation attack in data formats;
- Principles and methods for performance assessment of presentation attack detection algorithms or mechanisms;
- Classification of known attacks types (in an informative annex).

Work has started for Presentation Attack Detection (PAD) in 2011 by the Technical Committee ISO/TC JTC1, SC 37, Biometrics, WG3.

Two basic types of presentation attacks are distinguished:

- An **Active Imposter Presentation Attack** – subversive data capture subject intends **to be recognized as an individual other than him/herself**. Two subtypes:
  - The attacker intends to be recognized as a specific individual known to the system;
  - The attacker intents to be recognized as any individual known to the system, without specification as to which one.

- **An Identity Concealer Presentation Attack** – subversive data capture subject intends **not to be recognized as any individual known to the system**. Two subtypes:
  - The attacker will seek later repeatability of the disguised or altered biometric characteristic;
  - The attacker will seek no later use of the characteristic (a "one-time" deception).

Status as of 28/05/2015:

- ISO/IEC 30107-1 Biometrics presentation attack detection –Part 1 Framework: DIS (Draft International Standard);
- ISO/IEC 30107-1 Biometrics presentation attack detection –Part 2 Data formats: CD (Committee Draft);
- ISO/IEC 30107-1 Biometrics presentation attack detection –Part 3 Testing and Reporting: NP (New Project).

Follow-up discussions were starting as from 22 to 26 June 2015 and beyond.

5.4.1.3 Other standardisation efforts

The Common Criteria working groups (since 2000) worked on adaptation of the evaluation scheme for the evaluation of fingerprints based systems.

National schemes (FR, ES, DE) have been established since 2007. Particularly the Spanish CCN works on the definition of a document for:

- Defining the attacks to be taken into account during an evaluation;
- Defining a testing methodology;
- Defining a rating table for quantification of the resistance level.

The German BSI has created a Protection Profile (based on adapted Common Criteria norm up to EAL2+ level). This profile is limited to FP sensors, and uses a defined and large set of fake fingers. The MorphoSmart™ Optic 301 fingerprint reader has passed this evaluation.

The Biometrics Institute has developed a framework (BVA) to assess the vulnerabilities in biometric systems. Since 2007, it has been applied to face, finger and iris biometrics. It aims to address:

- Finding unknown vulnerabilities in systems;
- Providing different levels of vulnerability assurance;
- Assessing he full chain of security, including databases as well as sensors.

5.4.1.4 Performance challenges – ICE, MBGC, NICE, LivDet

The main performance challenges include: ICE 2005, ICE 2006, MBGC 2007-2009, NICE 2007-2009 and NICE II 2009-2011. However these were not specifically addressing spoofing.

From an anti-spoofing perspective, the **Liveness Detection (LivDet) Competitions – which** compare biometric liveness detection methodologies, are more relevant. They define a standardized testing protocol for:

- Large quantities of spoof and live samples;
- Software-based or system-based biometric liveness detection solutions.

LivDet competitions were hosted in 2009, 2011, 2013 and will be held during 2015. Currently LivDet is being hosted for iris and fingerprint liveness detection methods.

Available reports as of today are the Fingerprint reports of 2009, 2011, 2013, and the iris 2013 report.

5.4.1.5 The FP7 Tabula Rasa project

The TABULA RASA project addressed some of the issues of direct (spoofing) attacks on trusted biometric systems. Some academic publications are available through the traditional publishing channels.

However, the reports that are specifically focussing on spoofing are not publicly disclosed.

5.4.1.6 Iris attack methods

Documented iris attack methods include:

- Artificial eye;
- High quality print-out of the iris image;
- Using iris image as mask on a real eye (fights liveness detection by measuring pupil dilation);
- Cosmetic contact lenses (used for enrolment by one person and authentication by another person);
- Display of an iris image on a handheld screen.

Various attacks are described in [Ruiz2008], They report FAR of 0,1% and FRR of 12,71%, success rates observed around 50 % for different attack scenarios (iris print enrolled/verified, live iris enrolled/print iris verified).

5.4.1.7 Counter spoofing for iris - FastPass project

We summarise below the key points from 'Biometrics in ABC: counter-spoofing research' [FASTPASS]:

- **Optical properties** from different parts of an eye and retina reflection. High quality cameras are required for capturing these features;
- Galbally et al. (2012): liveness detection system based on a **set of image quality** related features;
- Chen et al. (2012): **texture changes of the conjunctival blood vessel** and **iris patterns** from **multispectral images**;
- More recently, Connel et al. (2013) proposed an approach to detect cosmetic contact lenses by **projecting additional structured light patterns onto the eye**;
- Image texture analysis, e.g. analysis of **high-frequency spectral** magnitude based on Fourier transforms (Daugman 2003). The method recognizes spurious coherence from printed iris patterns;
- Combinations: (Lee and Son 2012) **combined both optical and texture features** in iris anti-spoofing detection.

5.4.1.8 Counter spoofing for iris – Tabula Rasa

From those publications that are in the public domain, we selected the following statements as they provide relevant information:

[Galbally1]

It is possible to construct a synthetic image for a FAR = 0,0001%, reconstructed images have almost 75% chance of positively to the original real image.

It is possible to generate multiple synthetic iris patterns with iriscodes very similar to the real one. In 42,9% of all cases, 5 all reconstructed images were positively matched to the original real image.
Reconstructed images are less efficient in fooling humans. For trained people, the FAR and FRR lie around 10%.

[Galbally2]

This article proposes a two-stage protection scheme against masquerade attacks carried out with synthetically reconstructed iris images (as explained in [Galbally1]):

- Step 1: Edge detection: The number of edge pixels detected outside the iris boundaries;
- Step 2: Power spectrum analysis: The synthetic images have an abnormal amount of high-frequency energy compared to real irises.

This protection is effective against the attack described in [Galbally1]:

- The false genuine rate (ferrfake) = 0% (the rate of images that are falsely classified as genuine);
- The false rejection rate (ferrlive) = 0,3% (mostly due to bad quality of what was synthetically reconstructed).

5.4.1.9 Iris spoofing countermeasures – conclusions based on literature

Iris spoofing countermeasures are reasonably well addressed in the academic literature and a subject of much focus.

However it can be concluded that today there is no 'Silver Bullet' - not a single technology stands out as the 'silver bullet' iris-spoofing countermeasure. Different technologies address different attack vectors.

Standardisation of vulnerability assessment and certification of iris sensors for their anti-spoofing capabilities has been considered but has not been significantly advanced at this stage.

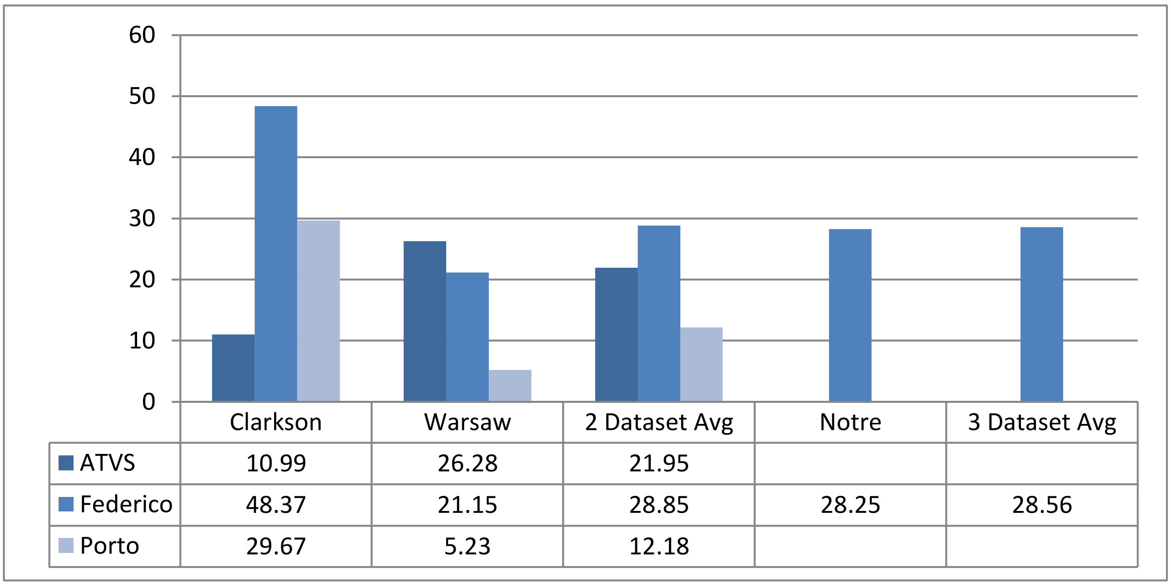
5.4.1.10 Iris liveness detection competitions

The 'LiveDet 2013 Iris Liveness Detection Competition' was held with following participants:

- ATVS - Biometric Recognition Group, ATVS Universidad Autonoma de Madrid;
- University of Naples Federico II;
- Faculdade de Engenharia Porto.

The dataset used for the evaluation contained images from 3 different datasets. Spoof images were collected using:

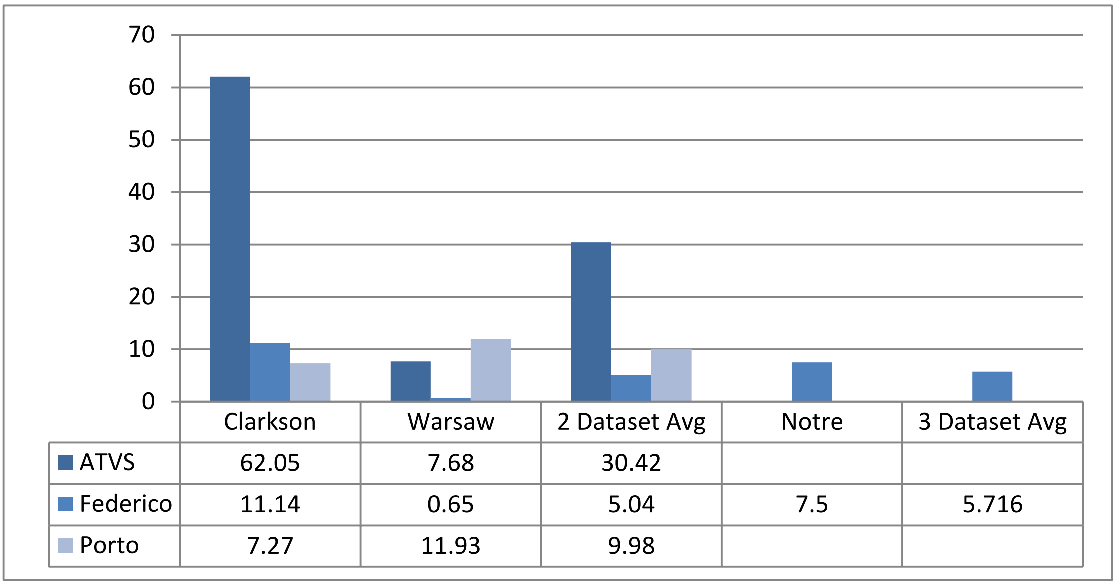
- Patterned contact lenses that obscure the natural iris pattern;
- Printed iris spoofs which aim to identify as another person.



	Clarkson	Warsaw	2 Dataset Avg	Notre	3 Dataset Avg
■ ATVS	10.99	26.28	21.95		
■ Federico	48.37	21.15	28.85	28.25	28.56
■ Porto	29.67	5.23	12.18		

Figure 67 *Rate of misclassified live iris images for submitted algorithms*[43]

[43] *Source: LivDet 2013 Iris Liveness Detection Competition 2013*



	Clarkson	Warsaw	2 Dataset Avg	Notre	3 Dataset Avg
■ ATVS	62.05	7.68	30.42		
■ Federico	11.14	0.65	5.04	7.5	5.716
■ Porto	7.27	11.93	9.98		

Figure 68 *Rate of misclassified spoof iris images for submitted algorithms*[44]

5.4.1.11 FP spoofing

The spoofing and anti-spoofing of fingerprints has a long history. Common spoofing attacks include:

- Scanned finger images;
- Artificial fingers and fingertip covers;
- Cadaver fingers.

Spoofing and countermeasures are reasonably well documented and discussed by the German CCC (Chaos Computer Club).

Counter measures include:

- In hardware – odour, pulse, blood pressure, temperature, electrical resistance, multi-spectral imaging, ultrasound;
- In software - image analysis;
- Or a combination of both.

Evidence suggests that combinations of measures from one or more categories should perform better than any single measure (Barsky et al 2012).

The 'LiveDet 2013 FP Liveness Detection Competition' for FP was structured into two parts:

- Part 1 Algorithms, where 11 algorithms tested against dataset generated from 4 different devices, with at least 4000 images from each device, half of the spoof images were collected in cooperative mode, the other half in non-cooperative mode;
- Part 2 Systems where 2 systems (Dermalog and Morpho) were tested against the dataset.

[44] *Source: LivDet 2013 Iris Liveness Detection Competition 2013*

For the algorithms:

***Table 18** Rate of misclassified live fingerprints (ferrlive) for submitted algorithms*[45]

	Biometrika	Italdata	Crossmatch	Swipe	Average
Dermalog	3.30	0.50	99.84	3.82	26.86
Anonym1	1.50	0.50	86.96	N.A.	N.A.
ATVS	4.60	0.00	90.40	0.00	23.75
Anonym2	2.30	0.20	98.40	2.52	25.85
UniNap1	30	2.10	31.28	11.45	11.96
UniNap2	1.80	5.00	55.20	33.22	23.80
UniNap3	1.80	2.10	55.20	11.45	17.64
Anonym3	3.30	1.00	95.52	2.69	25.63
HZ-JLW	65.30	26.10	100.00	25.33	54.18
Itautec	1.10	1.30	64.96	N.A.	N.A.
CAoS	5.50	21.10	41.92	N.A.	N.A.

***Table 19** Rate of misclassified fake fingerprints (ferrfake) for submitted algorithms*[46]

	Biometrika	Italdata	Crossmatch	Swipe	Average
Dermalog	0.10	1.10	0.00	3.20	1.1
Anonym1	2.40	1.70	2.40	N.A.	N.A.
ATVS	5.50	100.00	10.30	100.00	53.95
Anonym2	1.30	1.00	0.30	9.60	3.05
UniNap1	6.40	4.90	31.10	16.10	14.62
UniNap2	11.30	13.90	48.30	19.50	23.25
UniNap3	11.30	4.90	48.30	16.10	20.15
Anonym3	8.10	4.60	0.10	8.20	5.25
HZ-JLW	0.60	0.20	0.00	3.50	1.07
Itautec	16.90	6.50	13.90	N.A.	N.A.
CAoS	3.70	70.70	54.20	N.A.	N.A.

***Table 20** Rate of accuracy for submitted algorithms*[47]

	Biometrika	Italdata	Crossmatch	Swipe	Average
Dermalog	98.30%	99.20%	44.53%	96.47%	84.63%
Anonym1	98.00%	98.85%	50.53%	N.A.	N.A.

[45] *Source: 'LivDet 2013 Fingerprint Liveness Detection Competition 2013'-report*

[46] *Ibid.*

[47] *Ibd.*

ATVS	94.95%	50.00%	45.20%	53.55%	60.93%
Anonym2	98.20%	99.40%	45.20%	94.19%	84.25%
UniNap1	95.30%	96.50%	68.80%	85.93%	86.63%
UniNap2	93.45%	90.55%	47.87%	73.15%	76.26%
UniNap3	93.45%	96.50%	47.87%	85.93%	80.94%
Anonym3	94.30%	97.20%	46.89%	94.75%	83.29%
HZ-JLW	67.05%	86.85%	44.44%	84.81%	70.79%
Itautec	91.00%	96.10%	57.73%	N.A.	N.A.
CAoS	95.40%	54.10%	52.62%	N.A.	N.A.

For the Dermalog and Morpho systems:

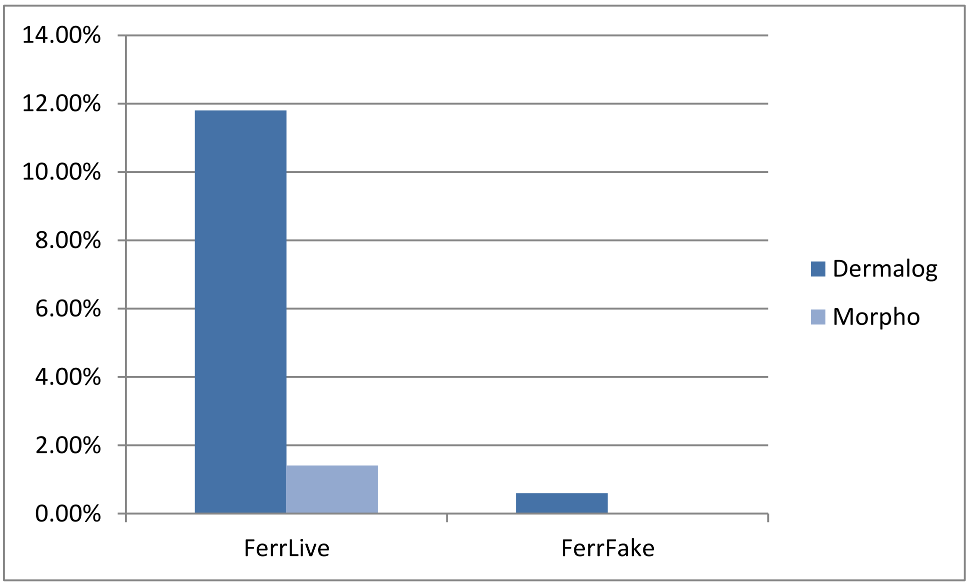


***Figure 69** FerrLive and FerrFake for submitted systems for Dermalog and Morpho*[48]

It can be observed that the Morpho system had a Ferrfake of zero %.

5.4.1.12 FI spoofing

A falsified face can be a printed photograph, a photograph or video displayed on a screen or some form of mask, make-up or cosmetic surgery.

The three main categories of counter-spoofing measures are:

- Motion analysis: based on the difference between motions in planar objects and real human 3D faces, HTER 9% (Anjos, 2011);
- Texture analysis, e.g. frequency component analyses (up to 100% effective, Li, 2004), local binary patterns (HTER ~15%, Trefny 2010);

[48] *Ibid.*

- Liveness detection: based on eye blinking, lip movements, temperature (dual camera) etc. e.g. blinking, 96% accurate (Pan, 2007).

In the context of the FastPass project[49], following observations can be made:

- MODI (Modular Digitis GmbH) developed anti-spoofing measures based on a Near Infrared (NIR) camera and multi-wavelength/multi-spot illumination;
- In the FastPass Newsletter #7 (Spring 2015), following detection rate for FI spoofing were claimed:
  - For iPad, iPhone and similar: 100%;
  - For spoofing an image on paper or texture: 97%.

The Newsletter claims these countermeasures can be executed while the subject is in motion, except for mask detection, where the subject has to stand still for a minimum of 5 seconds.

Furthermore, [SEC2DFACE] describes the '2nd Competition on Counter Measures to 2D Face Spoofing Attacks', 2013. The database used for Replay-Attack face spoofing consists of short video recordings of both real-access and attack attempts to 50 different identities. Three types of attacks are analysed: printed photographs, photographs displayed on the screen of a device and videos replayed on the screen of a device. Divided into 2 groups with regards to the support the attack media is attached to when they are presented to the system: fixed (the attack media is attached on a fixed stall) and hand (the attacker holds the attack media with his/her hands).

Table 21 *Performance results for the proposed anti-spoofing algorithms (in %)*[50]

	Development			**Test**		
Team	**FAR**	**FRR**	**HTER**	**FAR**	**FRR**	**HTER**
CASIA	0.00	0.00	0.00	0.00	0.00	0.00
IGD	5.00	8.33	6.67	17.00	1.25	9.13
MaskDown	1.00	0.00	0.50	0.00	5.00	2.50
LNMIIT	0.00	0.00	0.00	0.00	0.00	0.00
MUVIS	0.00	0.00	0.00	0.00	2.50	1.25
PRA Lab	0.00	0.00	0.00	0.00	2.50	1.25
ATVS	1.67	0.00	0.83	2.75	21.25	12.00
Unicamp	13.00	6.67	9.83	12.50	18.75	15.62

The ranking of the participating anti-spoofing algorithms is based on Half Total Error Rate (HTER). It is defined as a mean of False Acceptance Rate (FAR) and False Rejection Rate (FRR).

[49] For further details please see www.fastpass-project.eu

[50] Source: 'Second Competition on Counter Measures to 2D Face Spoofing Attacks 2013'

Table 22 *HTER of each countermeasure applying the intra-test (D1=D2) and the inter-test (D1≠D2) protocol*[51]

Countermeasure	**Train/Tune**	**Test**	**HTER (%)**		**HTER degradation (test set)** between D1=D2 and D1≠D2
	EER in D1	D2	Dev	Test	
Correlation	Replay EER=11.66%	Replay CASIA	11.66 47.72	11.79 48.28	309.50%
	CASIA EER=26.65%	Replay CASIA	50.23 26.65	50.25 30.33	65.68%
$LBPTOP^{u2}_{8,8,8,1,1,1}$	Replay EER=8.17%	Replay CASIA	8.17 60.00	8.51 61.33	620.68%
	CASIA EER=21.59%	Replay CASIA	48.97 21.59	50.64 23.75	113.22%
$LBP^{u2}_{8,1}$	Replay EER=14.41%	Replay CASIA	14.41 57.32	15.45 57.90	274.75%
	CASIA EER=24.63%	Replay CASIA	44.97 26.43	47.05 23.19	102.89%

Table 23 *HTER variation of each countermeasure applying the intra-test (D1=D2) and the inter-test (D1≠D2) protocol*[52]

Countermeasure	**Test**	**$Q_{R,C}$**	**HTER (%)**		**HTER degradation (test set) compared with "intra-set" protocol**	**HTER improvement (test set) compared with "inter-test" protocol**
			Dev	Test		
Correlation	Replay CASIA	0.11 -0.14	13.71	12.39 32.08	5.09% 5.77%	75.34% 33.55%
$LBPTOP^{u2}_{8,8,8,1,1,1}$	Replay CASIA	0.24 -0.41	23.16	26.04 38.18	205.99% 60.75%	48.58% 37.75%
$LBP^{u2}_{8,1}$	Replay CASIA	0.38 -0.41	19.69	21.66 47.16	40.19% 103.36%	53.96% 18.55%

5.4.1.13 Comparing modalities

The first comparison of modalities that was made publicly available was performed in 2000 by the UK CESG. The UK's CESG compared performance evaluation of seven biometric systems. . Tests were conducted by the NPL over the period May to December 2000 [CESG01]. They addressed FTE, FTA, FAR, FRR, but not spoofing. While old, this report provides a good starting point to compare the various modalities.

[51] Source: 'Second Competition on Counter Measures to 2D Face Spoofing Attacks 2013'

[52] *Ibid.*

Short name	Brief description
Face Face (2)	Visionics – Face It Verification Demo Alternative enrolment and matching algorithms for this system
FP-Chip FP-Chip (2)	VeriTouch – vr-3(U) Alternative enrolment and matching algorithms provided by Infineon
FP-Optical	Fingerprint recognition system
Hand	Recognition Systems – HandKey II
Iris	Iridian Technologies – IrisScan system 2200
Vein	Neusciences – Biometrics – Veincheck development prototype
Voice	OTG – SecurPBX Demonstration System

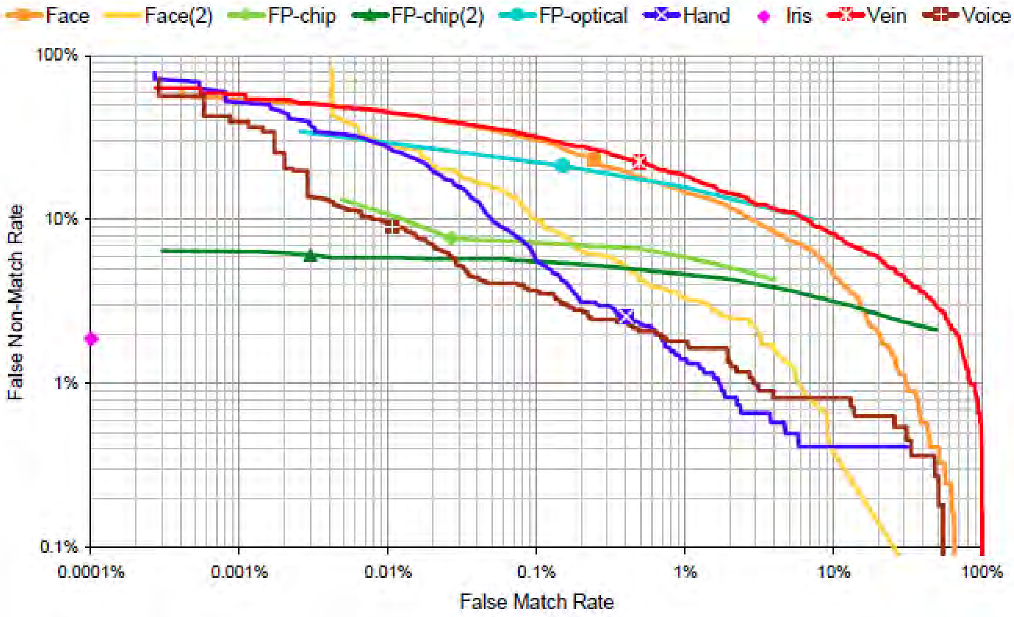


Figure 70 *Performance of biometric systems*

The performance is shown on a Detection Error Trade-off (DET) curve, which plots detection errors (False Match Rate against False Non-Match Rate) as function of the threshold. Typically, FMR is considered most important, and a low FMR is preferred. It can be observed that iris shows a permanent and very low FMR.

More recently, FRVT/ICE evaluation published the comparison below in 2006:

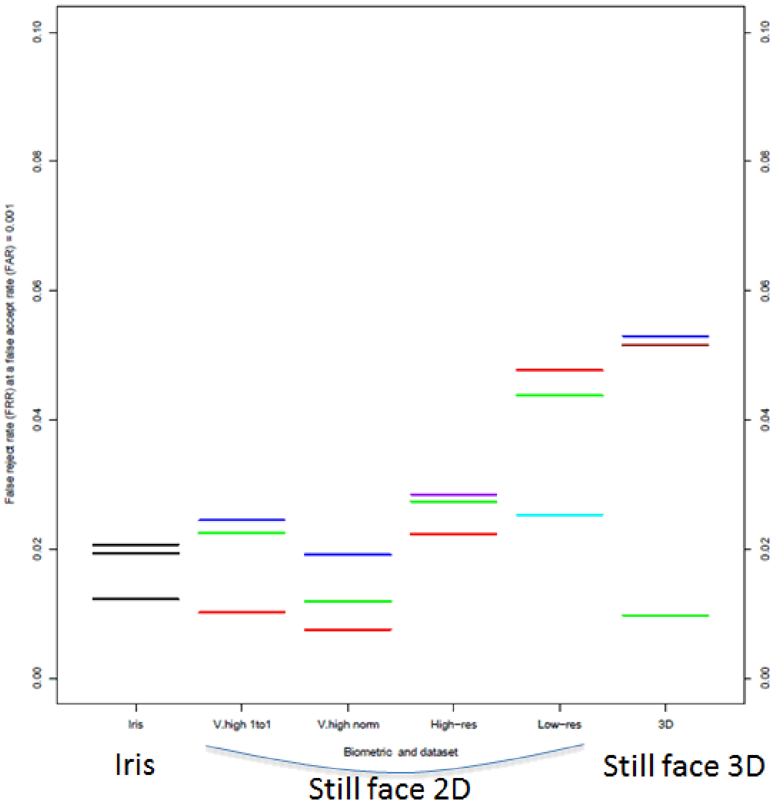


Figure 71 *Performance of biometric and dataset*[53]

All performance scores reported in this graph are FRR at a FAR of 0.001. The different colours indicate the different algorithms. Furthermore:

- The first column (labelled Iris) plots the median FRR for 3 evaluated iris algorithms;
- The second column (V.high 1to1) reports FRR for the top 3 one-to-one still face recognition algorithms on very-high resolution dataset;
- The third column (V.high norm) reports FRR for the top 3 normalized still face recognition algorithms on the very-high resolution dataset;
- The fourth (High-res) and fifth (Low-res) report FRR for normalized algorithms on the high-resolution and low-resolution datasets;
- The sixth column (3D) reports FRR for normalized 3D face recognition algorithms.

As can be seen on the figure above, under a fix FAR of 0,001, the differences between iris, and 2D face in FRR have become relatively small, and the security performance of these modalities has become roughly comparable.

We compare counter-spoofing measures and their effectiveness using Ferrfake (misclassified false acceptance) in the table below.

Table 24 *Comparison of counter-spoofing effectiveness*

[53] Source: FRVT 2006 and ICE 2006 Large-Scale Results - March 2007 – fig 10 p. 26

Iris (Livedet 2013)	FP (Livedet 2013)	FI (SEC2DFACE)
0.65% to 62.05%	1.07% to 53.95% across the individual algorithms	0.0% to 17.0% across the individual algorithms on 2D spoofing attacks
Average: 5.04%, 9.98% and 30.42% across two datasets	0% and 0.6% for systems	
Average: 5.7% across three datasets (the Federico algorithm was the only one evaluated over the three datasets)		

5.4.2 Findings

The answer to the question "Is iris enrolment more or less prone to spoofing and which anti-spoofing measures need to be taken?" is formulated in two parts as follows.

5.4.2.1 Is iris enrolment more or less prone to spoofing?

The most recent information we obtained in the public domain was from the LivDet2013 and SEC2DFACE competitions, which both published results in 2013. On the basis of this information, the counter-spoofing effectiveness of iris, FP and FI are of the same order of magnitude. This is illustrated by the comparable ferrfake (misclassified false acceptance) rates in ***Table 19***.

5.4.2.2 Which anti-spoofing measures need to be taken?

[Chapter to be finalised in Final Report – pending input from MS experts, Frontex and Biometric Institute]

5.5 Users' feedback

5.5.1 Border guards' feedback

11 border guards participated and replied to the survey from Lisbon airport**.** The **total number of replies received is of 27**[54].

The following dashboard presents a summary of replies[55].

[54] They reported on a weekly basis over 3 weeks. 6 questionnaires are missing because of holidays.

[55] Percentages are calculated per question and are based on the number of replies given. In some cases, BGs have given more than one reply to one question.

Overall feedback[56] ★ ★

Border Guard		Traveller
69 % felt more confident with equipment	74% rate the usability of equipment as good	79 % of replies indicated that travellers were mostly enthusiastic[57]

Potential improvement points

Border Guard		Traveller
41% of replies indicate either that iris process capture should be quicker or that the equipment should be placed closer	11 % of replies indicate that equipment could be more ergonomic	49% of replies indicate that more guidance to travellers could improve the process

Potential show-stoppers

Traveller	
Language 14%	Hardware problem 36%
-	Difficulty to use 9%
	Signal-system problem 5%

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- Difficulties experienced with iris capturing (as explained in section 5.6):
  - Light coloured eyes;
  - Senior travellers iris (over 60/65);
  - Tall people (over 1.85 m);
  - People need to keep their eyes wide open during the process, which is not always easy;
  - Process experienced as too lengthy.

[56] Rating: 3 * = good / 2* = neutral / 1* = weak.

[57] This is aligned with travellers' survey feedback showing 96.4% of satisfied or very satisfied answers for TC 5.

5.5.2 Travellers' feedback

The results collected ir ng positive reaction of the travellers. More thi

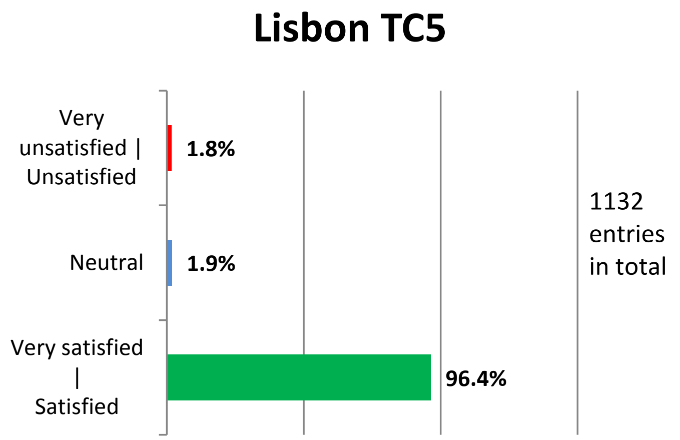


Figure 72 *Traveller satisfaction survey results for TC5 in Lisbon*

5.6 Constraints

5.6.1 Environmental conditions

The tests took place in Lisbon airport, with indoor conditions.

With the exception of some Border Guards citing the light coming from a glass wall at the back of the booths as a possible constraint at some time of the day during summer, no environmental conditions were noted as being constraints for the proper capture and verification of live facial images.

5.7 Feasibility

[To be added in the Final Report]

6. ABC gates

6.1 Introduction

[Treatment and cleaning of the data to be finalised for Final Report]

The increased use of ABC gates is a worldwide trend, with more and more countries deploying e-gates at various BCPs and enabling their use by passengers from different nationalities according to criteria set at national level.

By enabling automation of the most routine elements of the border crossing process and by accelerating low-risk border crossings, e-gates have been demonstrated to allow efficient handling of growing traveller numbers and of rational use of resources at the borders (FRONTEX, 2011).

The current requirements established within the Schengen Borders Code (SBC) provide for more extensive checks to be performed at entry (*i.e.* VIS check, ask questions to the passengers), thus limiting the possibilities of automation. For this reason, the Smart Borders Technical Study identified the possibility that e-gates be used only for exit checks of all TCNs having an e-MRTD.

The only condition would be that the e-gates use facial matching as a means to verify that the bearer of the travel document is its rightful owner (bearer verification). In this regard, the main challenges are related to the possibility of performing passive authentication of the e-MRTD of TCNs, ensuring that the facial image contained in DataGroup2 (DG2)[58] has not been altered.

Facial recognition is the principal biometric verification as most of the e-gates in Europe utilise facial recognition; moreover, the extraction of the FPs from the TCNs' passports would face significant challenges linked to the Extended Access Control (EAC). Nevertheless, the testing will also include ABC gates equipped with FP scanners, in addition to the facial image.

6.1.1 Objective

The possibility of TCNs using ABC gates at different border types has been assessed using the following metrics and structure:

1. **Operational and technical questions**
   a. Duration: What is the typical time for the automated border crossing
   b. Security: Is the authenticity of the Travel Document checked?
      - Quality indicators for the FI on the e-MRTD
      - Errors with e-MRTDs of TCNs
2. **Users' feedback**
   a. Perceived benefits by TCNs: Do travellers perceive a benefit in using e-gates?
   b. Perceived benefits by Border Guards: Do border guards perceive a benefit in having some TCNs use the automated exit paths provided that exit stamps would no longer be necessary? Benefits should relate in particular to workload.

[58] DG2 is one of the data group parts of the logical data structure of passport chip. DG2 stores the encoded face.

3. **Feasibility of the solution:**

a. Can automated exit checks of TCNs holding an e-MRTD be successfully applied?

6.1.2 ABC gates workflow

The use of ABC gates for exit checks is built upon five steps that permit judgement to be made on whether to allow passenger passage without manual intervention.

The process is divided into the following steps:

1) Passport authentication;

2) Capture of the facial image from the e-MRTD;

3) Enrolment of a suitable high-quality live facial image;

4) Verification of the facial image from the e-MRTD against the live facial image;

5) Stamping.

ABC gates can be categorised in two types: one step or two steps (integrated or not). Both of them have been tested during the Pilot.

6.1.2.1 Integrated two-step ABC gates

In an ABC system designed as an integrated two-step process, the traveller initiates the verification of the document and of the traveller's eligibility to use the system at the first stage, and then if successful moves to a second stage where a biometric verification (including the verification of the live FI against the image retrieved from the e-MRTD) and other applicable checks are carried out[59] (FRONTEX, 2012).

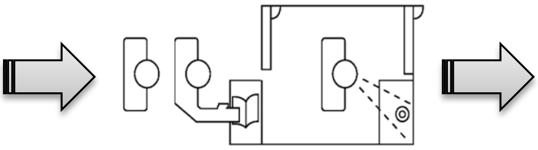


Figure 73 *Integrated two-step process with man-trap*[60]

6.1.2.2 One-step ABC gates

The verification of the traveller and the traveller's secure passage through the border are combined. This design allows the traveller to complete the whole transaction in one single process without the need to move to one section of the gate or man-trap to another stage[61] (FRONTEX, 2012).

[59] Source: Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, FRONTEX 2012.

[60] *Ibid.*

[61] *Ibid.*

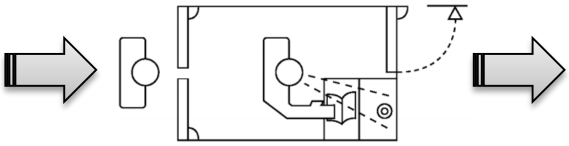


Figure 74 *One-step process with man-trap*[62]

6.2 Methodology

Existing e-gates located at five different BCPs[63] at exit have been adapted to also accept travelling with an e-MRTD. In addition, a new e-gate was set up at Gare du Nord specifically for the purpose of the testing. Stamping, where applicable[64], was provided once the TCN had passed the e-gate. All controls typically happening during the first line processing of passengers at exit controls were performed by the e-gates.

6.2.1 BCP selection

Below are the BCPs where the automated border controls for TCNs at exit (TC9) are carried out:

Air	Sea	Land
• Lisbon (PT)	• Helsinki (FI)	• Narva (EE)
• Schiphol (NL)		• Gare du Nord (FR)
• Charles de Gaulle (FR)		

As of 25 June, preliminary results from the Lisbon and Schiphol airports have been added to this chapter.

6.2.2 Configuration per BCP

This section outlines the main characteristics for the setup of the tests at the various BCPs. While assessing the results, it is important to keep in mind that even within the same vendors, the configurations of the ABC gates differ from one location to another. In some cases, different quality indexes and relative thresholds are used.

Each test instance defined the list of eligible nationalities, depending on the availability of the e-MRTD and of certificates. In both test instances, Lisbon and Schiphol, the nationality allowed in the testing were third countries for which the respective certificates were available.

[62] Source: Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, FRONTEX 2012
[63] In Narva the ABC gates had been installed just before the start of the tests
[64] If the person is in possession of a residence permit, then the stamping is not necessary

Table 25 *TC9 Lisbon airport – TC configuration*

Duration of the test	3 weeks (from 16.03.2015 to 03.04.2015)
Timetable of the tests	Monday to Friday – 8:00 to 17:00
Layout	One dedicated ABC gate at exit at Lisbon airport
Sample size achieved	1522[65]
Technical integration	Integrated
Integration within the regular border crossing process	Integrated
Equipment type	Existing integrated two-step ABC gate retrofitted to support TCNs' passports
Enrolment/verification threshold	Threshold based on verification matching score: 40[66] (vendor-specific index from 1 to 100)
Travellers' survey	Survey on a tablet after the test
Test personnel	Shifts of 2-3 border guards: 1 border guard in the booth doing stamping and final checks, 1-2 border guards recruiting volunteers and providing assistance if necessary

Table 26 *TC9 Schiphol airport – TC configuration*

Duration of the test	3 weeks (from 15.04.2015 to 08.05.2015)
Timetable of the tests	Weekday mornings– 8:00 to 12:00
Layout	Existing ABC gates adapted to be used also at exit - modification in the passenger flow/queue management
Sample size achieved	2304[67]
Technical integration	Integrated
Integration within the regular border crossing process	Integrated
Equipment type	Existing one-step ABC gates retrofitted to support TCNs' passports
Enrolment/verification threshold	Threshold based on verification matching score: 85[68] (vendor-specific index from 1 to 100)[69]
Travellers' survey	Survey on a tablet after the test
Test personnel	Shifts of 2 border guards: 1 border guard in the booth doing stamping and final checks, 1 border guard operating all the ABC gates, 2 hostesses

[65] Number of entries after data cleaning.
[66] Expected FAR and FRR ≈1%.
[67] Number of entries after data cleaning.
[68] Schiphol and Lisbon thresholds are equivalent (expected FAR and FRR ≈1%).
[69] The quality index scale is different between Lisbon and Schiphol.

6.2.3 Sample characteristics

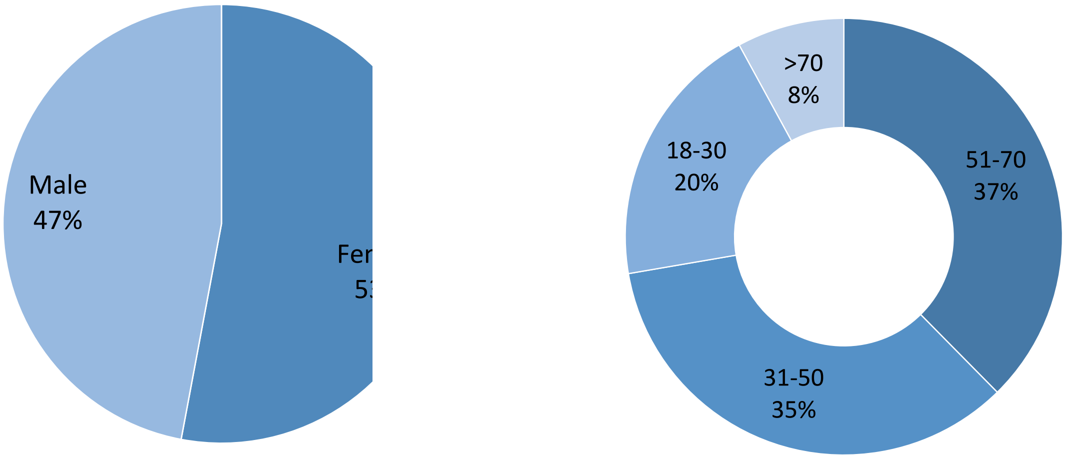


Figure 75 *TC9 Lisbon airport - Sample characteristics per gender and age*

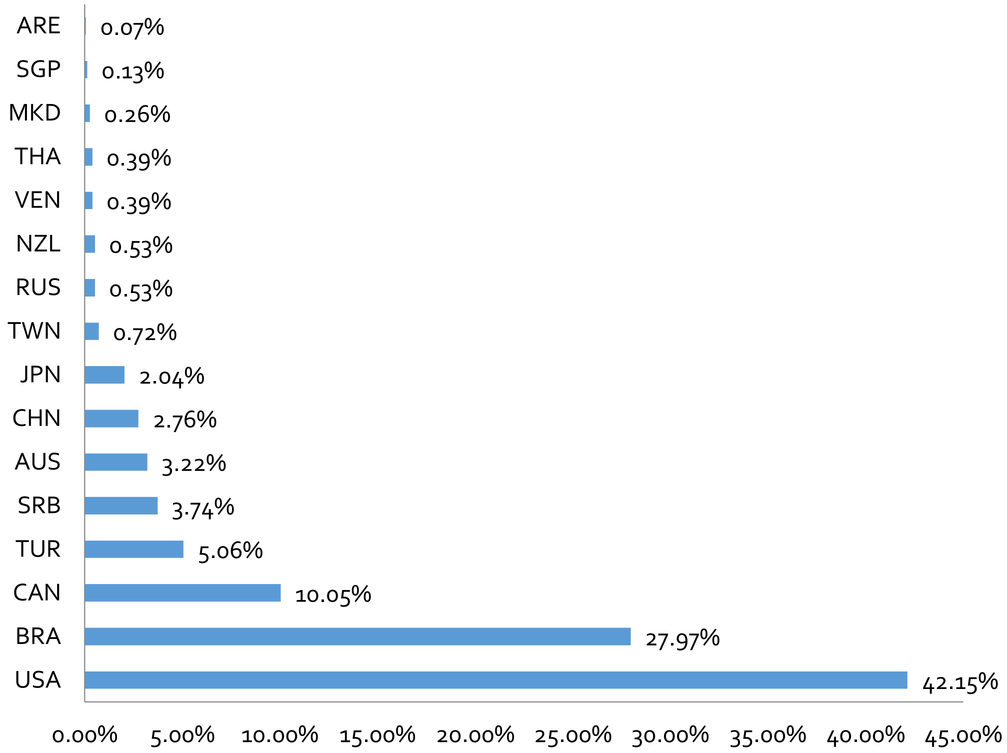


Figure 76 *TC9 Lisbon airport - Sample characteristics per nationality*

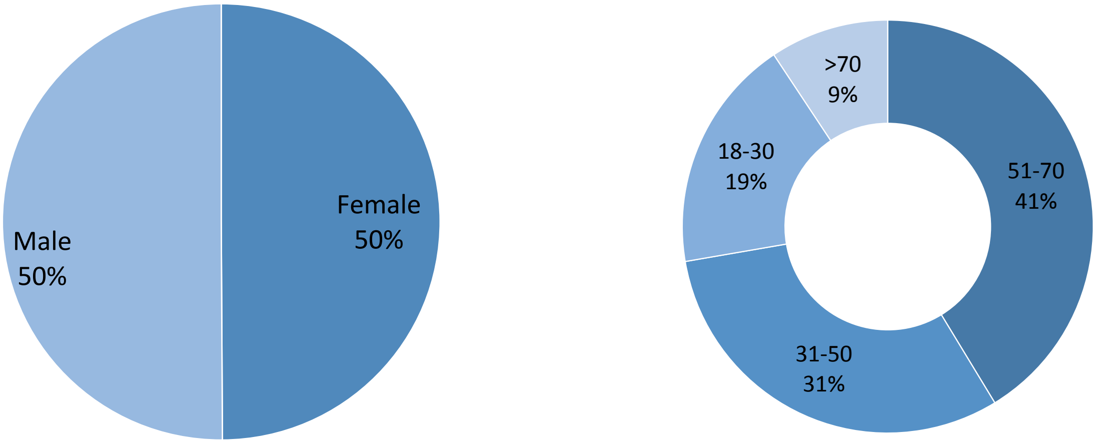


Figure 77 *TC9 Schiphol airport - Sample characteristics per gender and age*

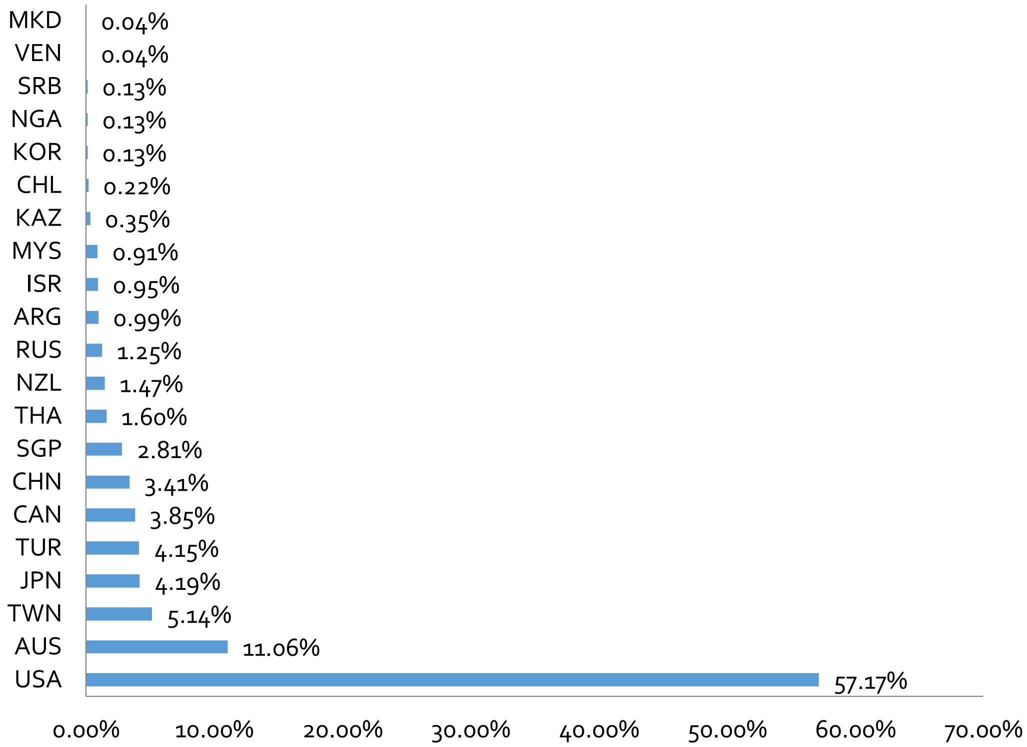


Figure 78 *TC9 Schiphol airport - Sample characteristics per nationality*

6.3 Technical and operational questions

6.3.1 Duration

Across the various operational tests executed within the Pilot, it was important to record the duration of border crossing using the different test setups.

The duration of each of the main individual steps making up the workflow at an ABC gate was recorded as well as the overall time necessary for a given person to pass through the ABC gate. As a final step, the latter end-to-end duration will be compared to that necessary to go through the border checks at a manual booth in order to assess the possible time savings linked to the introduction of ABC gates for TCNs.

6.3.1.1 ABC gate crossing time

This section describes the time it takes a given traveller to pass through the ABC gate. The duration was measured by using time-stamped log files produced by the ABC gate itself. The average crossing duration was calculated considering only those instances in which passive authentication (PA) was successful. If PA failed, the passenger could not transit the gate.

Measured from …	**…to**
The passenger starts interacting with the ABC gate by placing his/her passport onto the reader	The moment the man-trap opens to let the passenger through[70]

6.3.1.1.1 Lisbon

For 82% of travellers, transit through the ABC gates took less than 40 seconds, with 40% being able to cross in less than 20 seconds. In only 2% of the cases did the crossing exceed 60 seconds, with an absolute maximum of 110 seconds being noted for successful transit.

The median[71] and average times of transit were below 30 seconds (22 seconds and 27 seconds, respectively).

[70] Stamping is not calculated as part of this duration.

[71] The median is the number separating the higher half of a data sample from the lower half. Compared to the average value, it is more robust against extreme values.

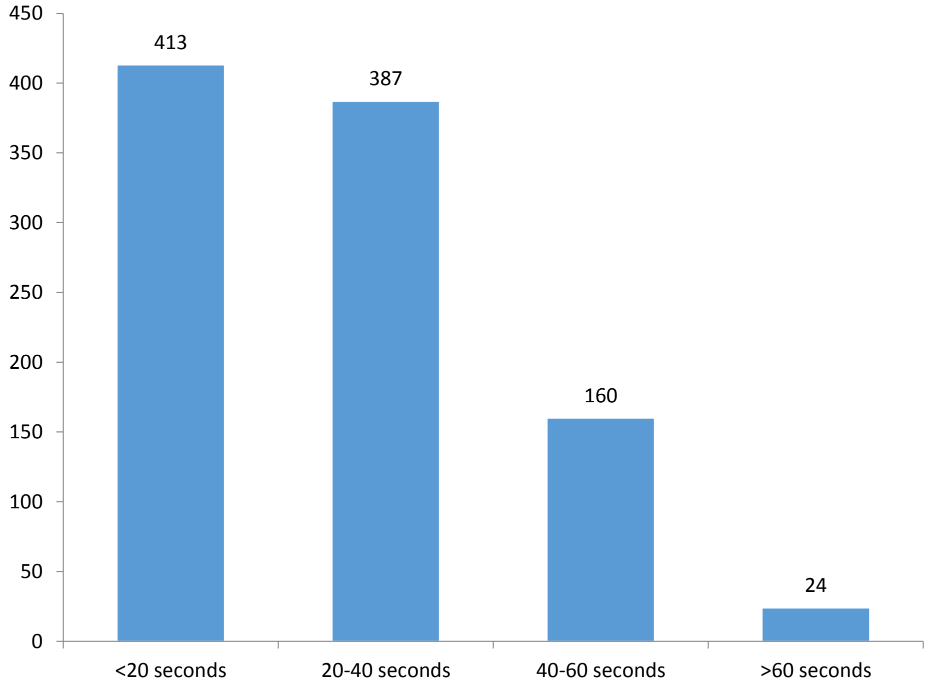


Figure 79 *TC9 Lisbon airport - Breakdown duration of e-gate transit*[72]

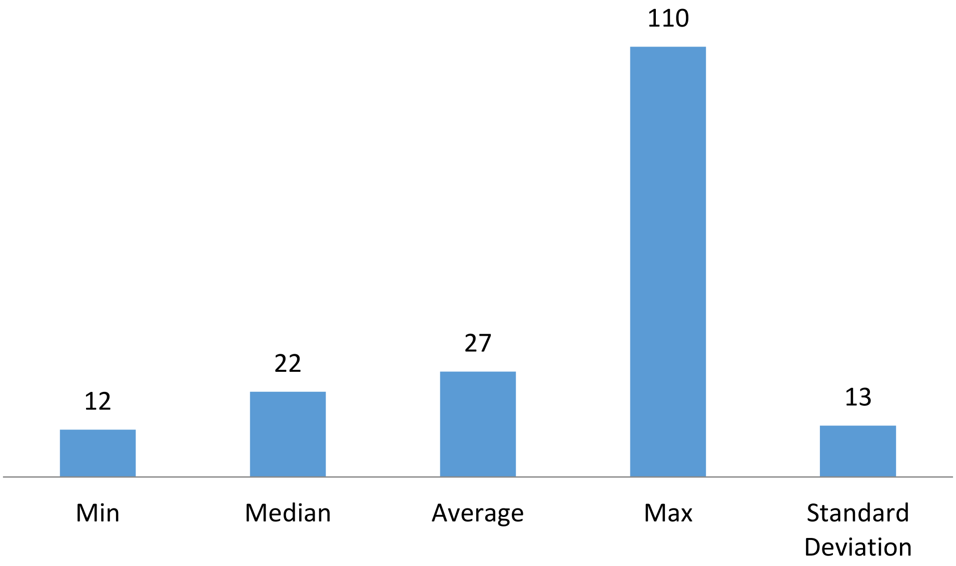


Figure 80 *TC9 Lisbon airport* ***-*** *Duration of e-gate transit*

6.3.1.1.2 Schiphol

Around 80% of the travellers were able to cross the e-gate in less than 20 seconds. Only 2.3% of the travellers took more than 40 seconds to go through the gate.

[72] Average calculated only if passive authentication was successful.

The one-step setup of the e-gate seems to allow a shorter duration for the transit. Section 6 will provide further details and greater granularity by analysing the workflow's individual steps.

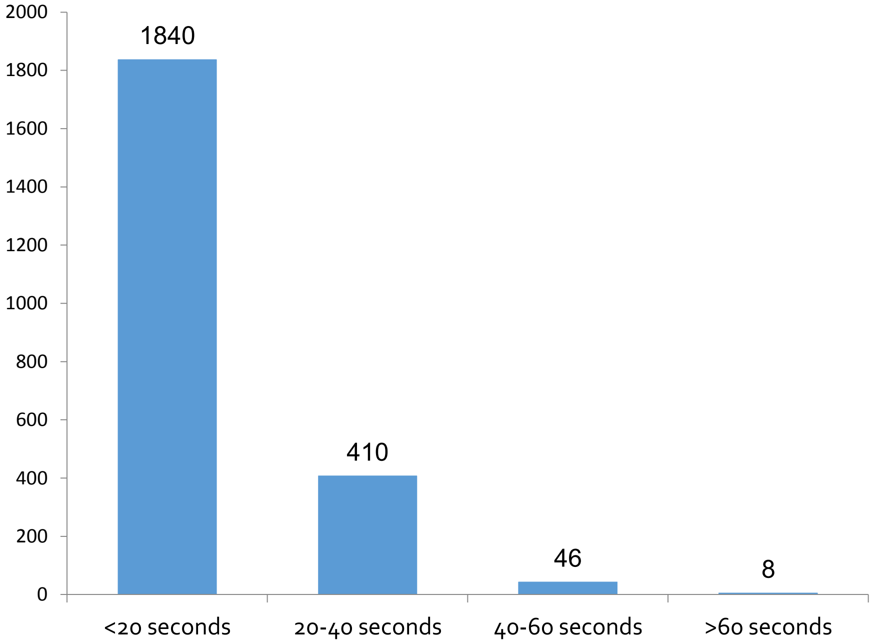


***Figure 81** TC9 Schiphol airport - Breakdown duration of e-gate transit*[73]

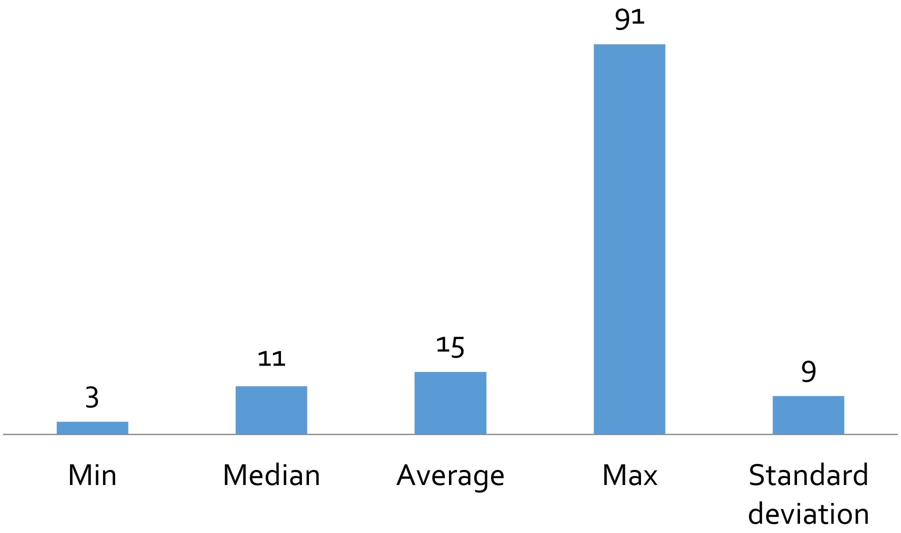


***Figure 82** TC9 Schiphol airport - Duration of e-gate transit*

6.3.1.2 Individual steps

In order to better explain the overall end-to-end durations introduced in the previous section and to explain the differences in durations observed at different locations, the time required to complete some of the

[73] Average calculated only if passive authentication was successful.

individual steps that together comprise the overall process of e-gate transit was recorded. Durations of a selection of relevant steps composing the workflow at an ABC gate have been analysed in order to provide more granularity on what makes up the overall time to cross an e-gate.

The information was collected using the time-stamped log files of the ABC gates. The steps considered were:

a Facial Image retrieval from the chip

Measured from …	***To …***
The first attempt at reading DG2	The successful capture of the facial image in DG2

b Passive Authentication

Measured from …	***To …***
The first attempt at performing passive authentication	The successful passive authentication

c Live image capture

Measured from …	***To …***
The first shot attempt	1. The successful capture; or 2. Camera system timeout

d Verification against the image captured from the e-MRTD chip.

Measured from …	***To …***
The first attempt at performing matching	Successful matching (above threshold)

Depending to the specific configurations of each e-gate, different steps may be performed in parallel. The analysis and comparison of the internal workflow of various e-gates goes beyond the scope of this report.

6.3.1.2.1 Lisbon

The chart below provides average durations for each of the main individual steps. Capturing the live facial image is the most time-consuming step, as it takes 15 seconds out of the total crossing time of 27 seconds on average.

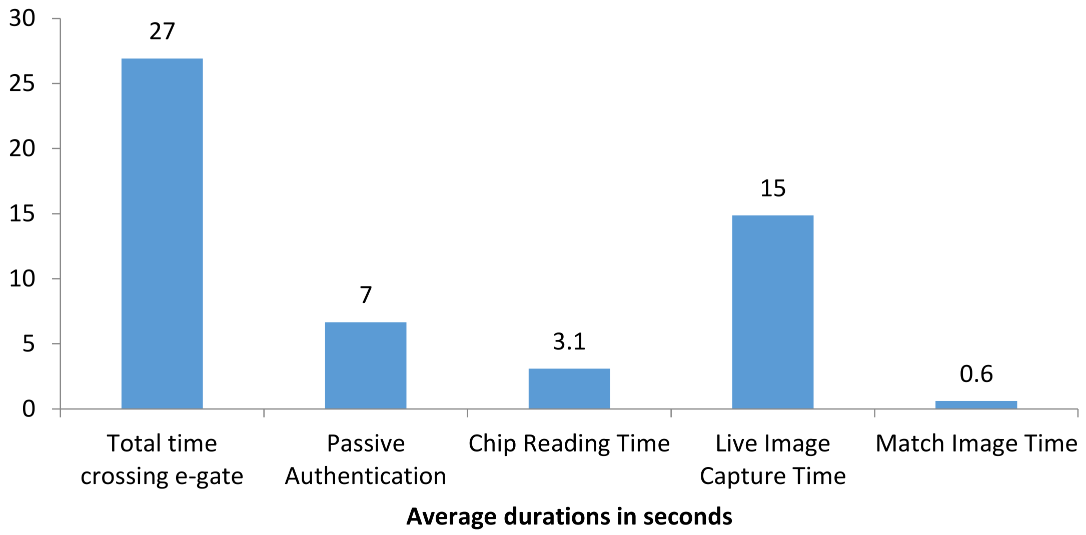


***Figure 83** TC9 Lisbon airport - Comparison of average values for the individual steps recorded*

a. Facial Image retrieval from the chip

The average time needed to retrieve the FI from the e-MRTD was 3.1 seconds. However, there are differences between the times required to retrieve the facial image from different national passports, as shown in Figure 84 below. Across the different nationalities passing through the test, the lowest average was 2.2 seconds and the highest was 5 seconds, as illustrated in the figures below.

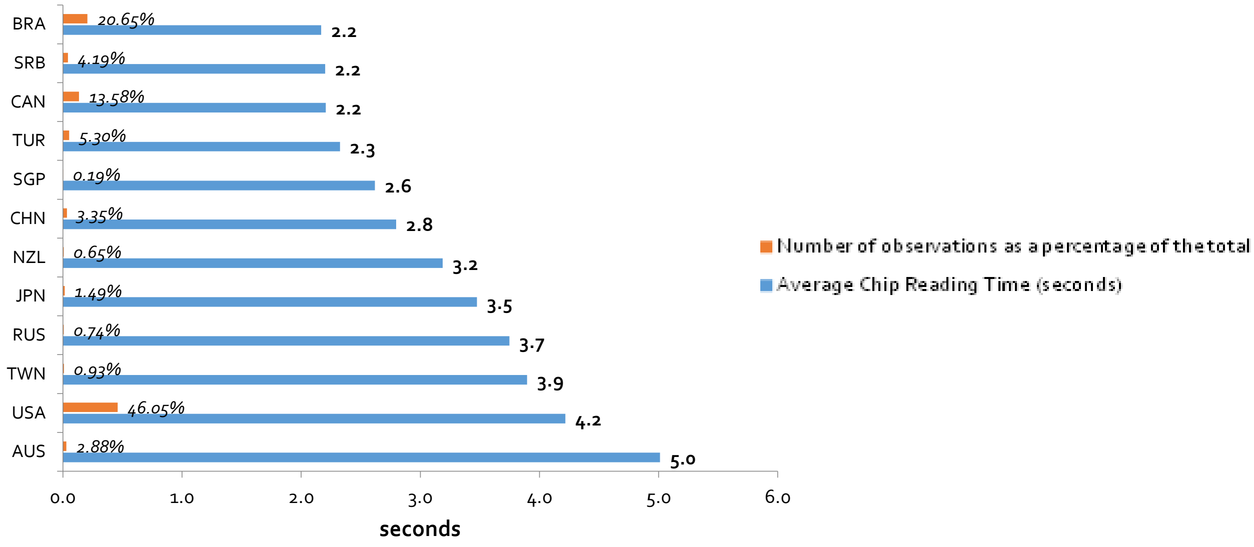


***Figure 84** TC9 Lisbon airport - Breakdown of the average time needed to extract the FI from the e-MRTD for each nationality*

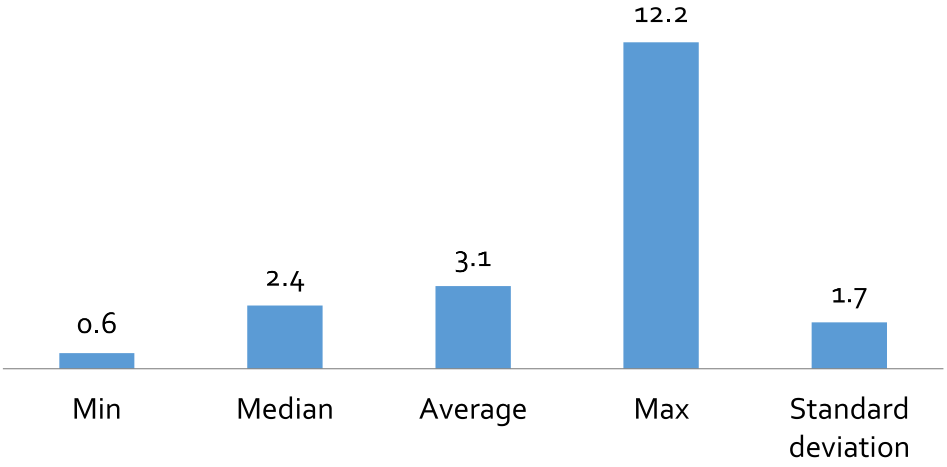


Figure 85 *TC9 Lisbon airport - Time needed to extract the FI from the e-MRTD*

b. Passive authentication

The graph below presents the time needed to perform passive authentication, when successful it was taking:

- Less than 5 seconds in 26% of cases;
- Less than 10 seconds in 88% of cases;
- More than 10 seconds in 12% of cases.

The median of the recorded values was 7 seconds.

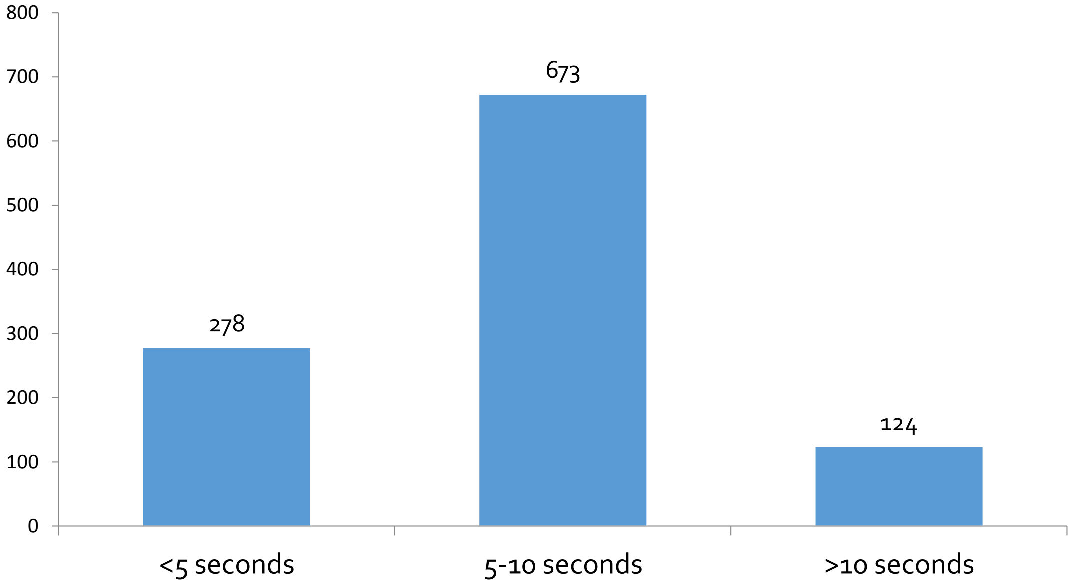


Figure 86 *TC9 Lisbon airport - Breakdown of the average duration of passive authentication*

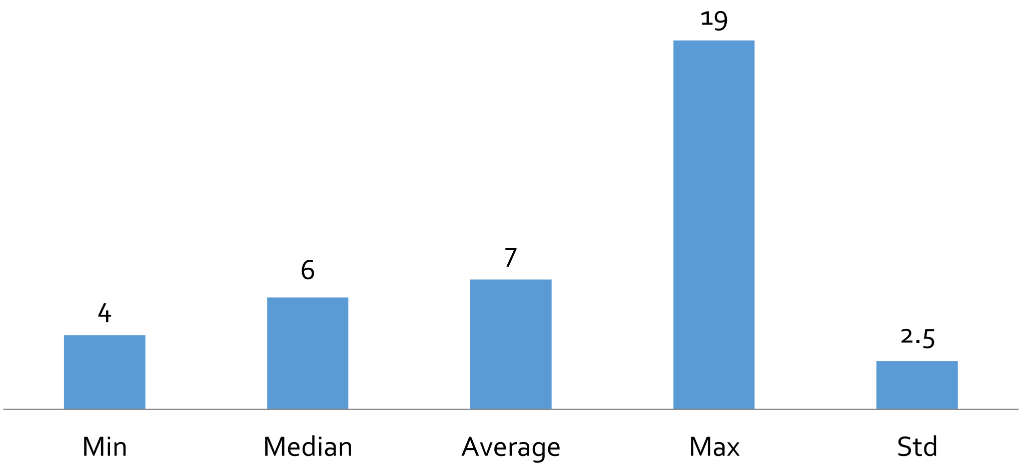


***Figure 87** TC9 Lisbon airport - Passive authentication time*

[Further investigation of the passive authentication time is currently ongoing]

c. Live image capture

The graph below presents the time needed to capture the live image, which was taking:

- Less than 10 seconds in 45% of cases;
- Less than 20 seconds in 73% of cases;
- 30 seconds (timeout time) in 19% of cases.

The median of the recorded values was 11 seconds.

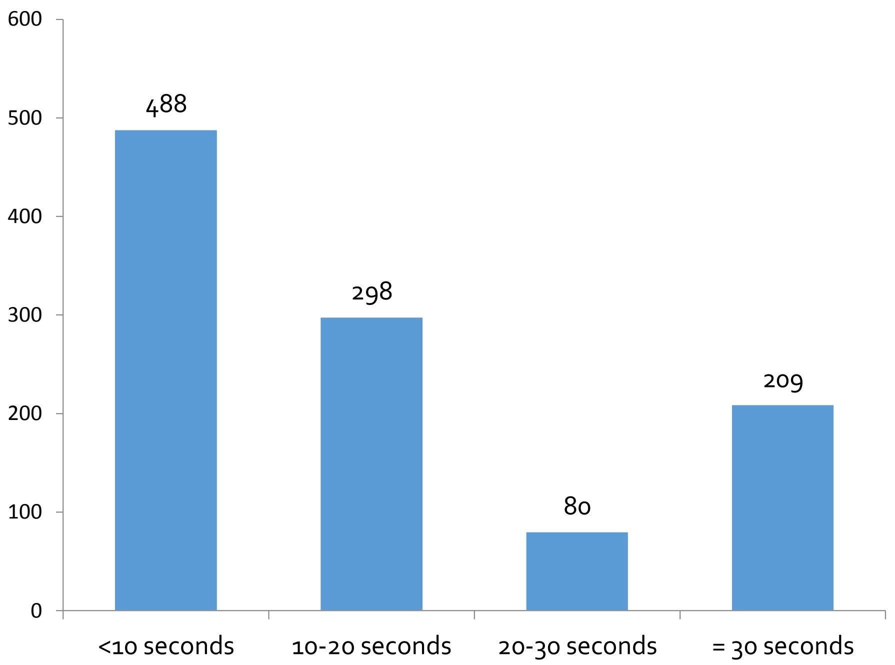


***Figure 88** TC9 Lisbon airport - Breakdown of the average live facial image capture*

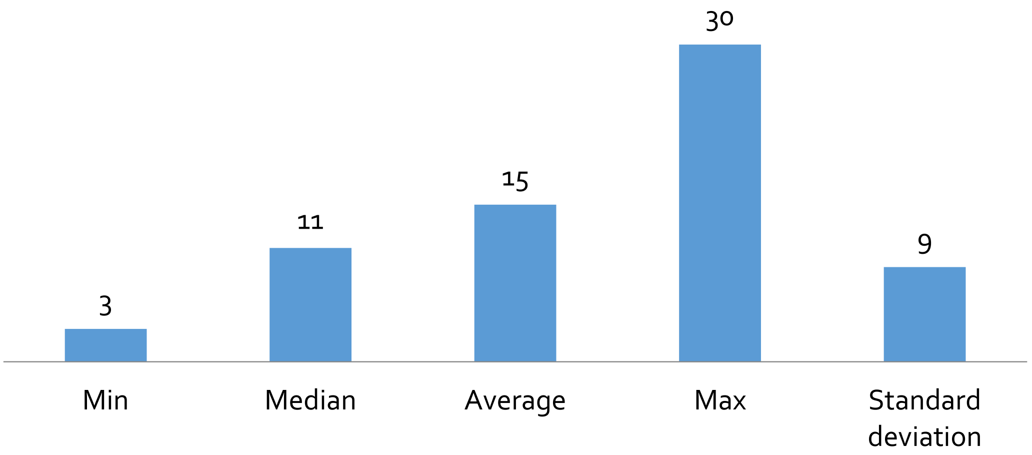


Figure 89 *TC9 Lisbon airport - Live facial image capture time*[74]

d. Verification against the image captured from the e-MRTD chip.

The time to perform the biometric verification was very short, being 1 second maximum with a median value of 0.6 seconds.

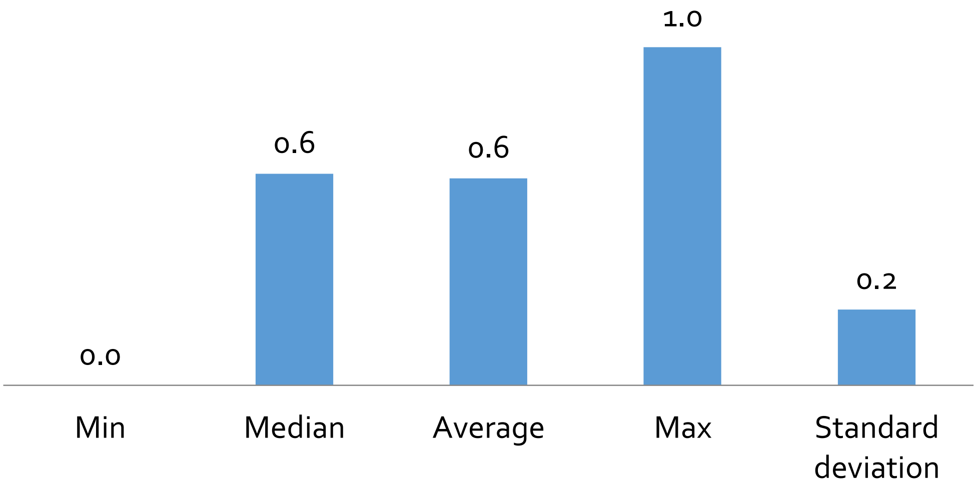


Figure 90 *TC9 Lisbon airport - Facial image verification time*

6.3.1.2.2 Schiphol

Figure 91 provides the average durations for each of the main individual steps. The one-step setup seems to be effective in shortening the duration of the live facial image capture, enabling an overall crossing time of just 15 seconds.

[74] The timeout for the live FI capture was set at 30 seconds.

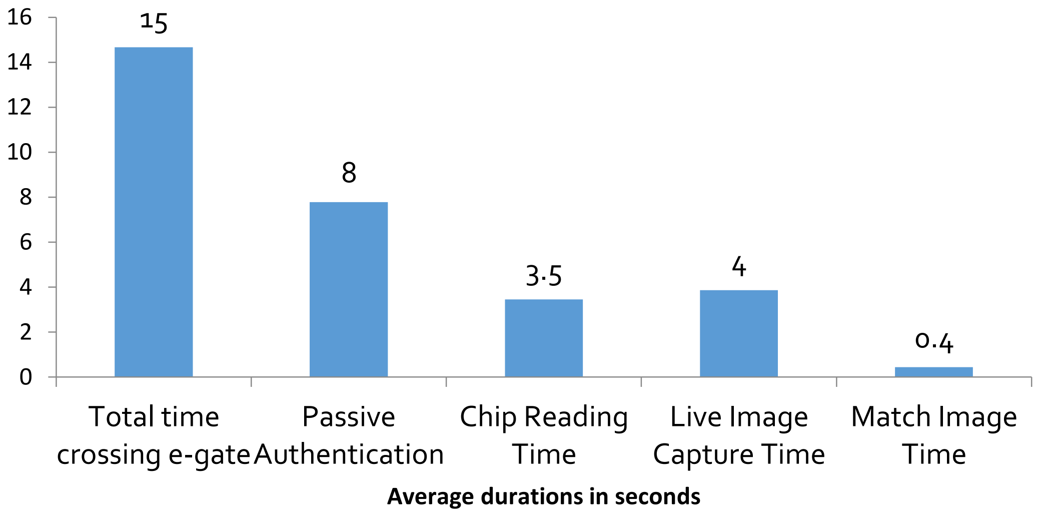


Figure 91 *TC9 Schiphol airport - Comparison of average duration for the individual steps recorded*

a. Facial Image retrieval from the chip

The average time needed to retrieve the FI from the e-MRTD is 3.5 seconds, with average values ranging from 2.1 to 3.9 seconds, depending on the nationality.

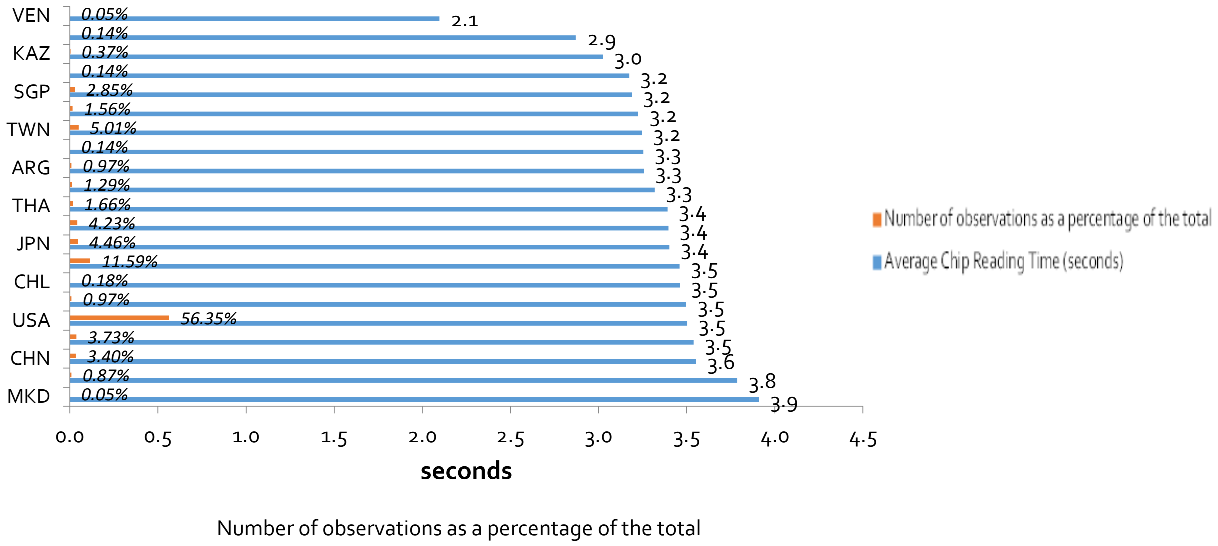


Figure 92 *TC9 Schiphol airport - Breakdown of the average time needed to extract the FI from the e-MRTD for each nationality*

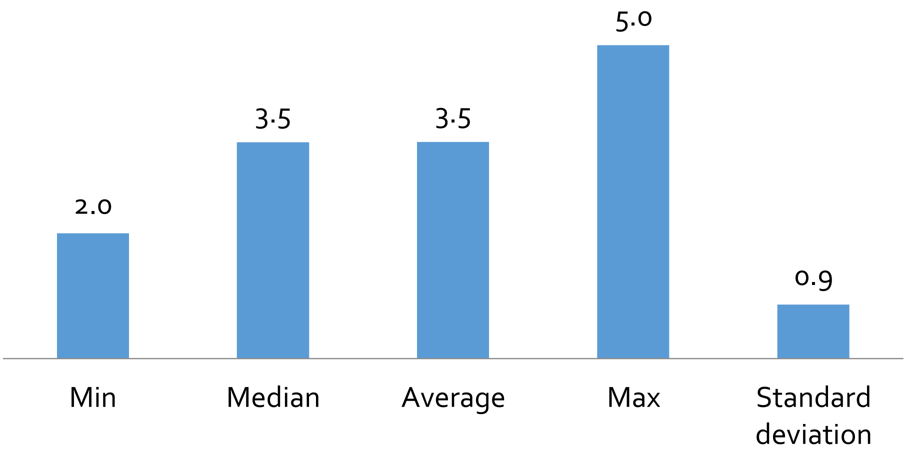


Figure 93 *TC9 Schiphol airport - Time needed to extract the FI from the e-MRTD*

b. Passive authentication

The graph below presents the time needed to perform passive authentication, when successful it was taking:

- Less than 5 seconds in 6% of cases;
- Less than 10 seconds in 85% of cases;
- More than 10 seconds in 21% of cases.

The median of the recorded values was 7 seconds.

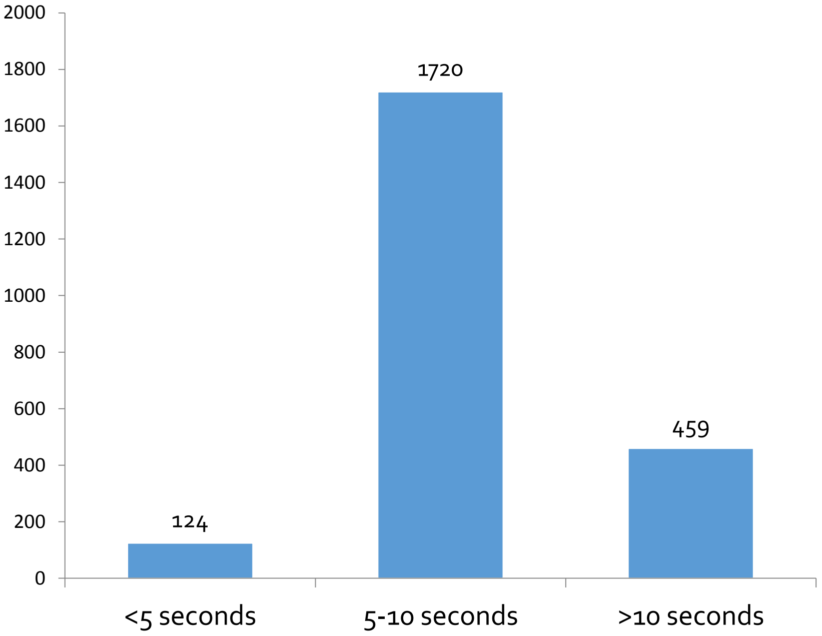


Figure 94 *TC9 Schiphol airport - Breakdown of the average duration of passive authentication*

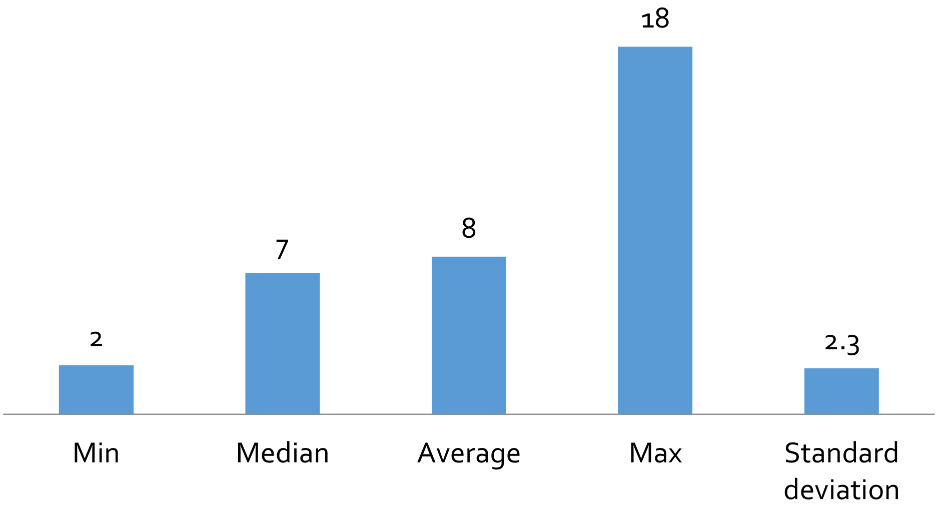


Figure 95 *TC9 Schiphol airport - Passive authentication time*

[Further investigation of the passive authentication time is currently ongoing]

c. Live image capture

The graph below presents the time needed to capture the live image, which was taking:

- Less than 5 seconds in 76% of cases;
- Less than 10 seconds in 84% of cases;
- 12 seconds (timeout time) in 14% of cases.

The median of the recorded values was just 2 seconds.

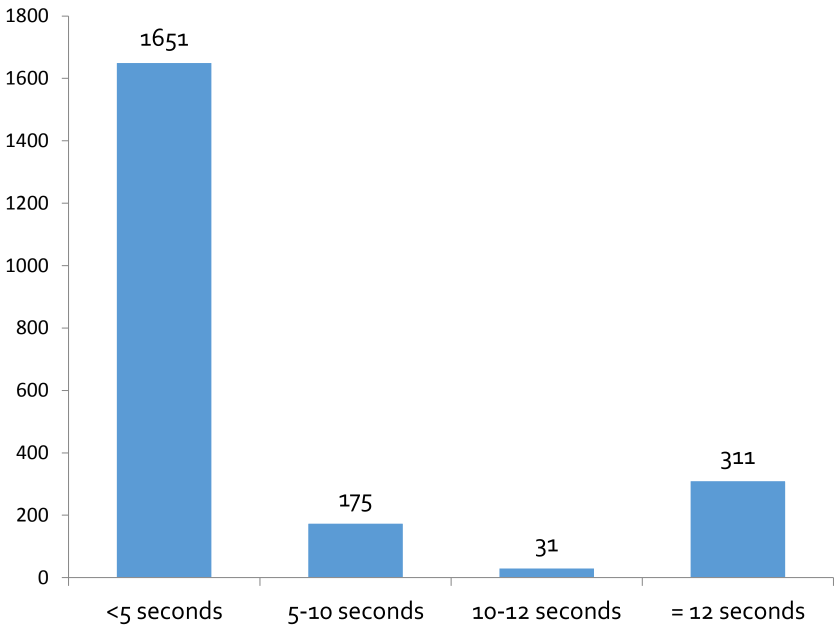


Figure 96 *TC9 Schiphol airport- Breakdown of the average live facial image capture*

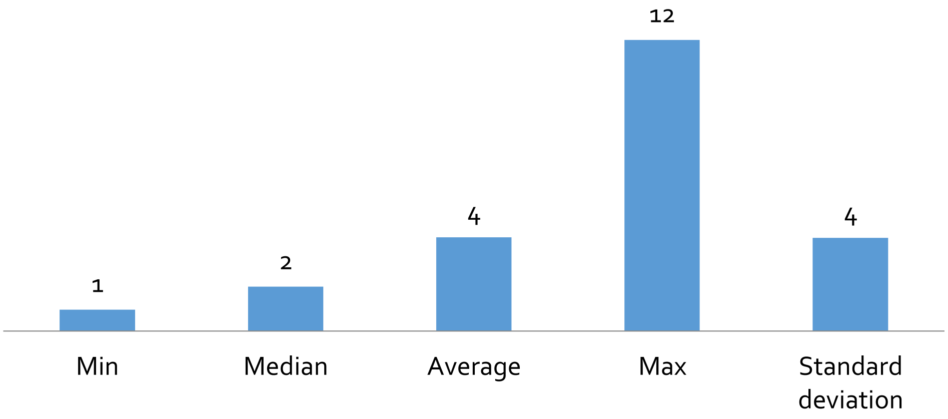


***Figure 97** TC9 Schiphol airport - Live facial image capture time*[75]

d. Verification against the image captured from the e-MRTD chip.

The time to perform the biometric verification was very short, being 1 second maximum with a median value of 0.4 seconds.

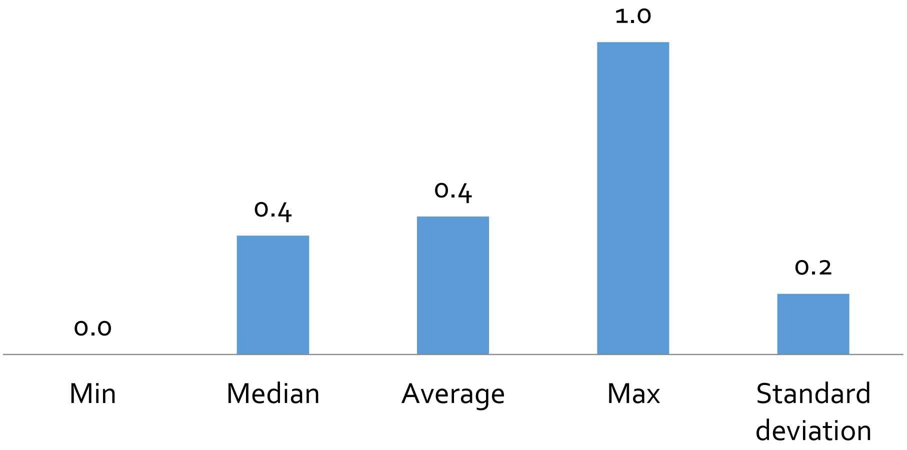


***Figure 98** TC9 Schiphol airport - Facial image verification time*

6.4 Security aspects for the use of ABC gates at exit

The majority of the e-gates installed in Europe rely on facial recognition; therefore, the extension of the use of ABC gates to TCNs would imply reliance on their facial images stored in the e-MRTDs for comparison against the live facial image in order to verify their identity.

[75] The timeout for the live FI capture in Schiphol was set at 12 seconds.

To ensure a sufficient level of security, three aspects were deemed to be worthy of further examination:

- **Quality of the FI stored on the e-MRTD:** it influences the verification performance;
- **Passive Authentication of TCNs' e-MRTDs:** verification of the integrity of the picture stored on the e-MRTD is crucial to ensure a sufficient level of security. For this purpose, passive authentication must be performed which implies that the operator has received the updated country signing (CSCA) certificates and/or Document Signer (DS) certificates for all the nationalities eligible for the ABC gates.

In addition, for ABC gates using FPs as additional biometrics, the following is also required:

- **Quality of the FPs captured:** the security performance of the FP verification directly depends on the quality of the capture that can be achieved at the e-gate.

[Further lessons and elements can be taken from TC4, 6, 7 including the work done on the chip desk research]

6.4.1 Quality indicators

In order to fill in the knowledge and experience gap that currently exists regarding use of the FI from non-EU passports, quality indicators for the facial image in each passport were recorded.

The measurement relies on vendor-specific quality indexes calculated assessing a sub-set of ICAO indicators and other elements (e.g. contrast, presence of glasses, head position, etc.). Having to rely on these proprietary indexes limits the possibility of comparing the data across different vendors and locations.

The information of the quality is complemented by the results of the FI verification, with failure to verify above the implemented thresholds indicating possible issues with the chip image quality.

Further data on the quality of the FI stored on e-MRTDs of TCNs can be found in chapter 4.

6.4.1.1 Lisbon

The quality scores for the FIs stored on the e-MRTDs scanned in Lisbon scored all in the second half of the range of the quality index, with an average value of 74[76] out of 100 (median value of 79). This evidence seems to suggest that while the average quality does vary depending on the nationality – as shown in the following chart – for all the passports examined, the quality of the picture was not critical.

[76] From the results for which passive authentication was successful.

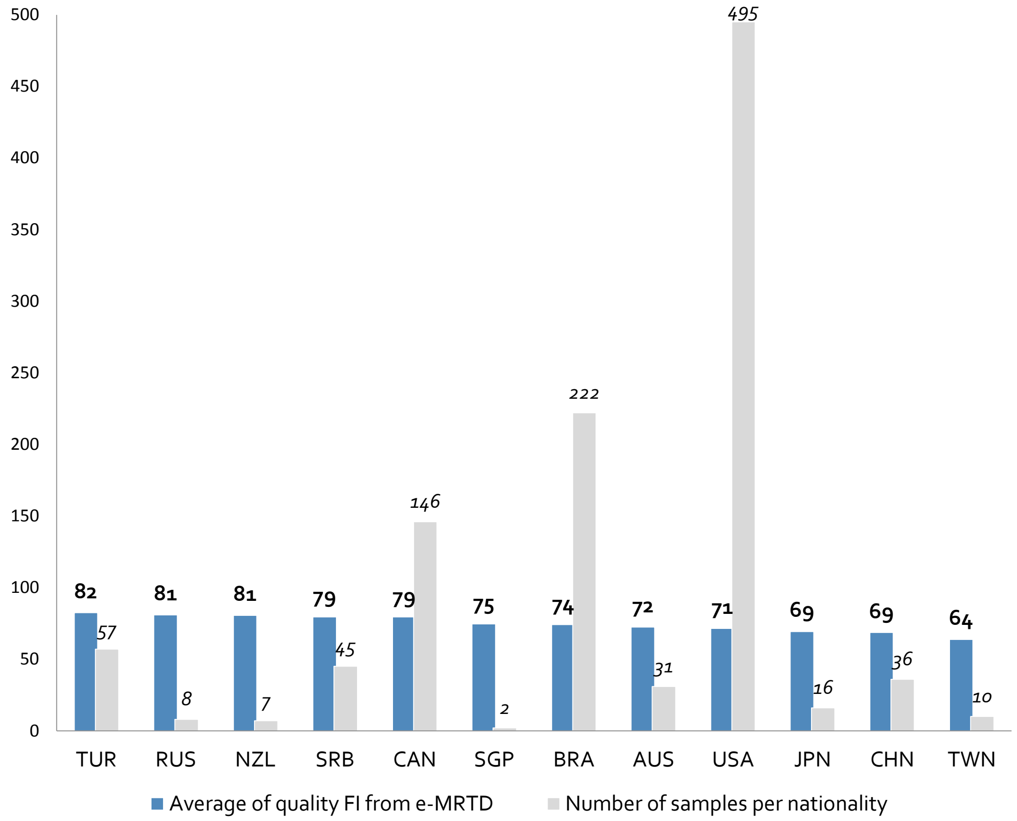


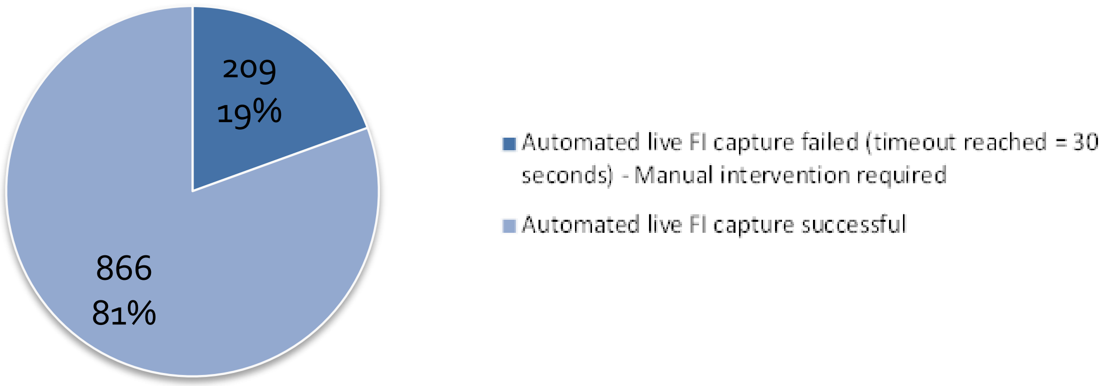
Figure 99 *TC9 Lisbon airport - Breakdown by nationality of the quality scores[77] of the FI on the chip[78]*

FI verification

The FI live capture results show that for 19% of the samples, the live capture would reach the timeout limit of 30 seconds. This means that the threshold for verification was not met.

[77] The vendor-specific quality index assesses a sub-set of ICAO indicators (based on the quality measures contained in ICAO Document 9303) and expresses the quality of the FI assessed on a scale of 1 to 100.

[78] Observations retained only if passive authentication was successful.



Automated live FI capture failed (timeout reached = 30 seconds) - Manual intervention required

Figure 100 *TC9 Lisbon airport- Breakdown of successful/unsuccessful automated FI capture and verification*[79]

Automated live FI capture successful

6.4.1.2 Schiphol

The quality scores from the FI stored on the e-MRTDs scanned in Schiphol scored all in the second half of the range of the quality index (*i.e.* above 50 out of 100), with an average value of 73 out of 100 (median value of 77).

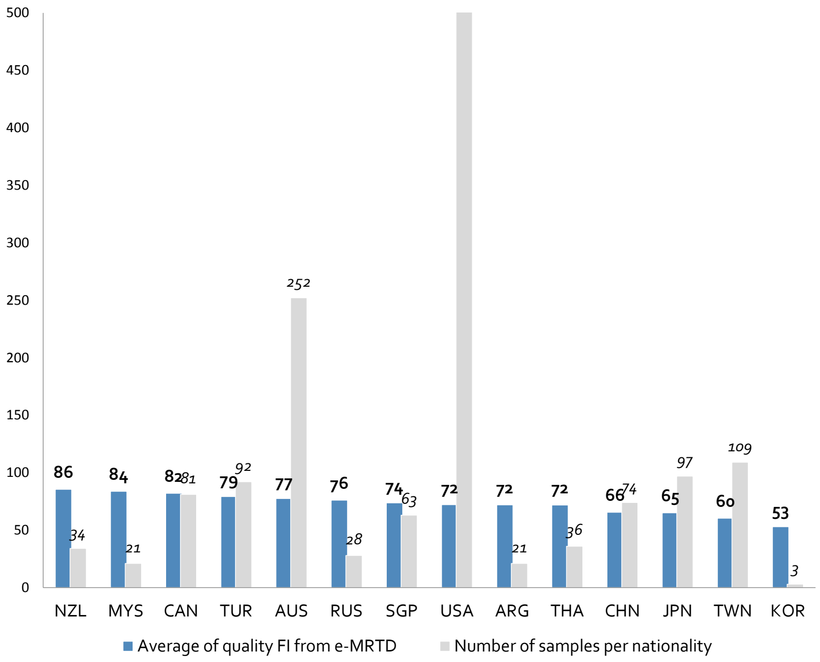


Figure 101 *TC9 Schiphol airport - Breakdown per nationality of the quality scores*[80] *of the FI on the chip*[81]

[79] If the live FI cannot be matched against the image from the e-MRTD.

FI verification

The FI live capture results show that for 12% of the sample, the live capture would reach the timeout time of 12 seconds.

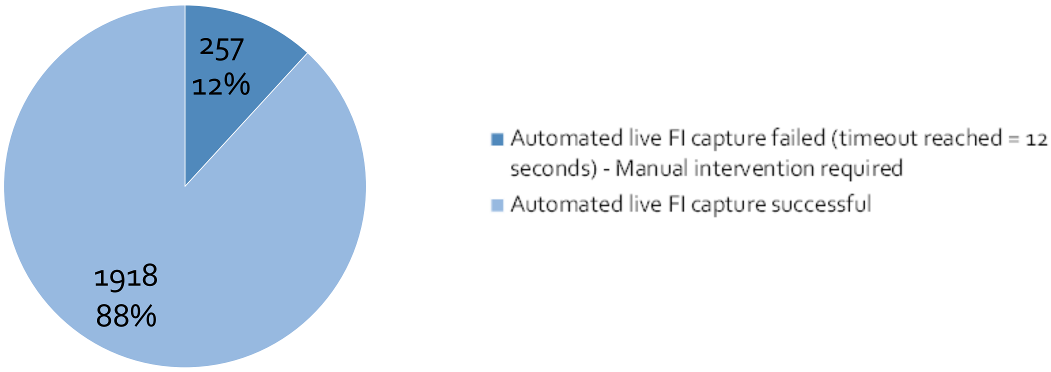


Figure 102 TC9 Schiphol airport - Breakdown of successful/unsuccessful automated FI capture and verification

6.4.2 Errors with e-MRTDs and Passive Authentication

In all ABC-focussed tests, errors encountered when reading e-MRTDs and during passive authentication have been recorded and analysed. These errors provide an insight into the issues and difficulties that could be expected if the pool of eligible nationalities for e-gates were expanded to also include TCNs.

Chapter 4.3 (TC6) further explores the issues and challenges of retrieving the FI from the e-MRTD of TCNs, by complementing the operational results with desk research.

It is worth noting that not all the errors recorded are necessarily due to technical issues; in some cases, they were caused by human error, *i.e.* the passport was removed during the reading process. It was not always possible to observe the difference from the logs retrieved, as the equipment cannot always distinguish whether the cause was technical or not.

6.4.2.1 Lisbon

The most frequent error noted was PA failure[82], occurring in 19% of all entries.

[80] The vendor-specific quality index assesses a sub-set of ICAO indicators and expresses the quality of the FI assessed on a scale of 1 to 100.

[81] Observations retained only if passive authentication was successful.

[82] Only nationalities (non-EU) for which the certificates were available could participate to the testing.

An ac he chip or
retrie

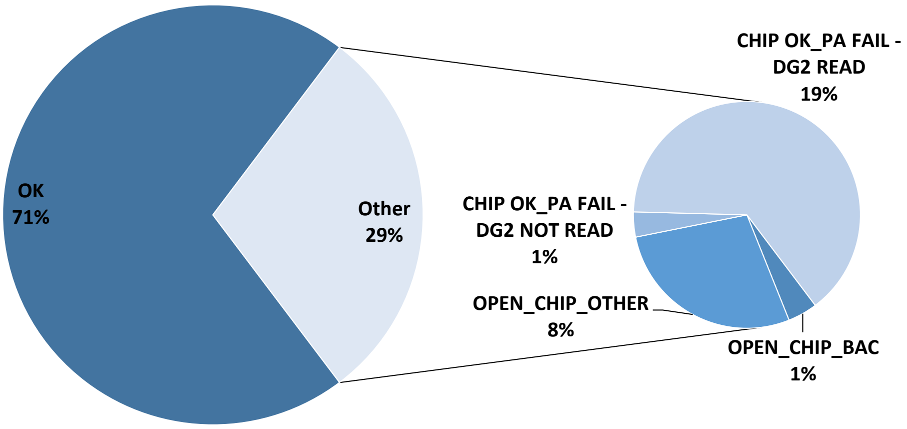


Figure 103 *TC9 Lisbon airport -Breakdown of error codes*[83]

One of the main reasons behind such high occurrence of errors with the PA, according to the observations recorded in Lisbon, was linked to problems with the Brazilian certificates, as Brazilian travellers are an important share of travellers at the Portuguese airport.

A high incidence of errors was also recorded with US passports, which, however, were also the most common nationality passing through the test.

[83] Error codes:

- OPEN_CHIP_BAC: error when attempting to perform the Basic Access Control;
- OPEN_CHIP_ERROR: generic error when attempting to access the passport chip;
- CHIP_OK_PA_FAIL–DG2 READ: error when attempting to perform the passive authentication. DG2 was successfully read;
- CHIP_OK_PA_FAIL – DG2 NOT READ: passive authentication error, DG2 could not be read.

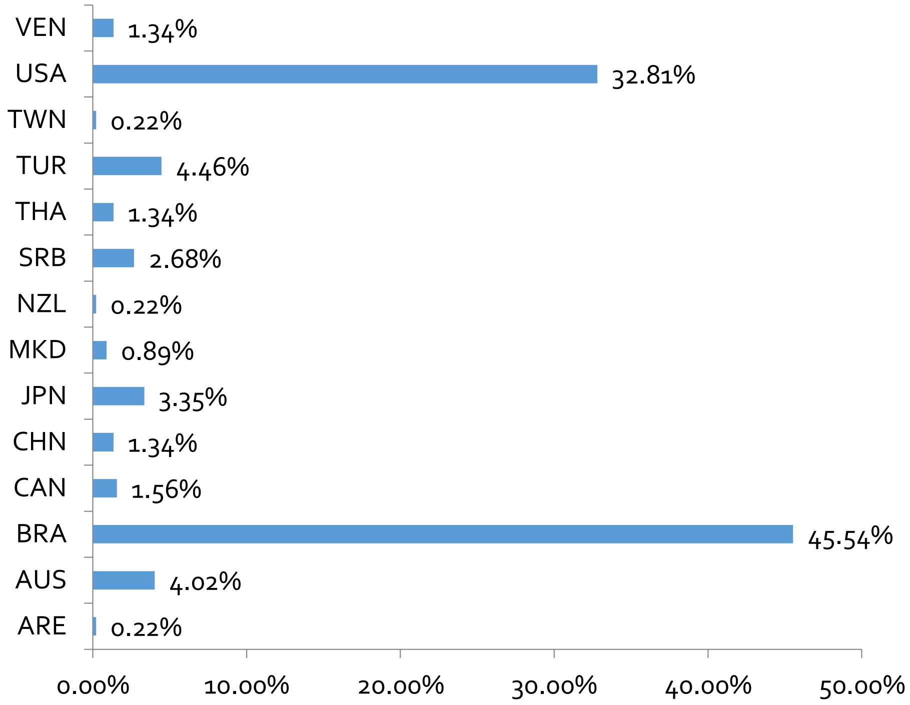


Figure 104 *TC9 Lisbon airport* **-** *Breakdown occurrence of error codes for each nationality (as a percentage of the total number of errors)*

6.4.2.2 Schiphol

[The error incidence and breakdown described within this section may change depending on some pending clarification for a small amount of data with outstanding issues to be assessed]

Only a limited number of errors has been registered through the testing period, equal to 6% of the total number of entries. US nationals had the highest number of errors; however, US nationals also made up the majority of the population going through this test instance (57% of the total population) [84].

[84] Only nationalities (non-EU) for which the certificates were available could participate to the testing.

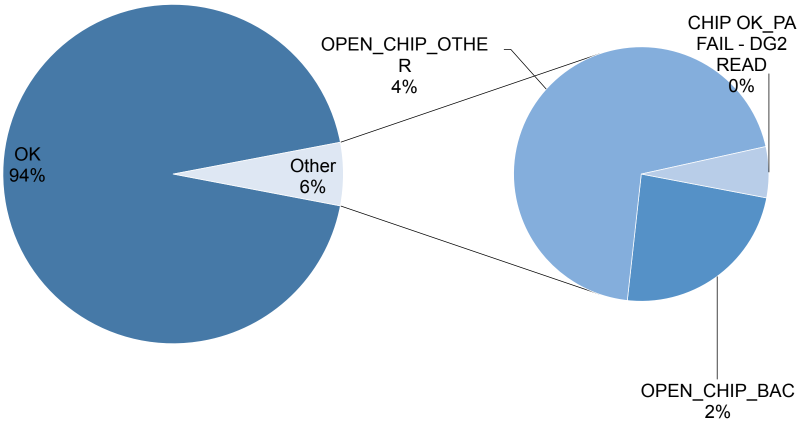


Figure 105 *TC9 Schiphol airport - Breakdown of error codes*[85]

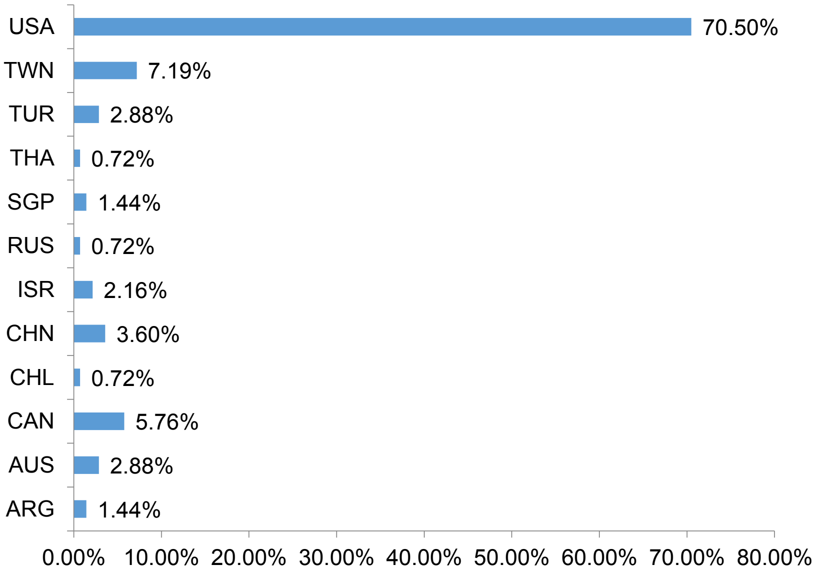


Figure 106 *TC9 Schiphol airport* **-** *Breakdown occurrences of error codes for each nationality (as a percentage of the total number of errors)*

[85] Error codes:

- OPEN_CHIP_BAC: error when attempting to perform the Basic Access Control;
- OPEN_CHIP_ERROR: generic error when attempting to access the passport chip;
- CHIP_OK_PA_FAIL–DG2 READ: error when attempting to perform the passive authentication. DG2 was successfully read;
- CHIP_OK_PA_FAIL – DG2 NOT READ: passive authentication error, DG2 could not be read.

6.5 Users' feedback

6.5.1 Border guards' feedback

6.5.1.1 Lisbon

11 border guards participated in and replied to the survey from Lisbon Airport **over a period of 3 weeks**. They reported on a weekly basis and the **total number of replies received was 29[86].**

The following dashboard presents a summary of replies[87].

Overall feedback[88] ★ ★ ★

Border Guard		Traveller
93% felt more confident with the equipment	93% rated the usability of the equipment as good	100% of replies indicated that travellers were mostly enthusiastic[89]

Potential improvement points

Border Guard		Traveller
Recurrent problems with chip reading have been identified (refer to chapter 4.8)	7% of replies indicated that the equipment could be more ergonomic	93% of replies indicated that more guidance to travellers could improve the process

Potential show-stoppers

Traveller	
Language barrier: 10%	Hardware problem
	Signal-system problem: 27%
	Difficult to use: 7% (chip reading issue)

[86] 3 BGs went on holiday and 1 could not answer the survey since software maintenance was ongoing.
[87] Percentages are calculated per question and are based on the number of replies given. In some cases, BGs have given more than one reply to one question.
[88] Rating: 3 * = good / 2* = neutral / 1* = weak.
[89] This is aligned with feedback from the travellers' survey, showing 94% of satisfied or very satisfied answers for TC 9.

Observations and preliminary conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- **Overall, experience with passengers was positive and some points for improvement were mentioned**:
  - Passengers liked the idea that they would save time at the border crossing;
  - Reluctance regarding written consent: some passengers (e.g. 5 out of 100 on the first day) refused to participate;
  - More information about the use of the system would ease the process for travellers.
- **Equipment:**
  - Mainly chip reading issues especially for Brazilian passports (as explained in chapter 4.8).

6.5.1.2 Schiphol

[Border guard survey results – missing at the time of writing – will be inserted in Final Report]

6.5.2 Travellers 's feedback

The results collected so far in Schiphol and Lisbon were very positive. Due to the placement of the tablet, only those TCNs that were able to cross the ABC gates, either with a successful automated FI verification or following the manual intervention of the border guards, were able to provide feedback. Travellers, whose e-MRTD could not be read or authenticated, could not reach the tablet and provide their feedback. However, technical issues with TCNs' passports are not specific to e-gates and thus the opinions of those who were able to use the e-gates were considered most relevant.

6.5.2.1 Lisbon

The results collected in Lisbon and summarised in the chart below show that travellers responded overwhelmingly positively. Less than four percent of the travellers were dissatisfied

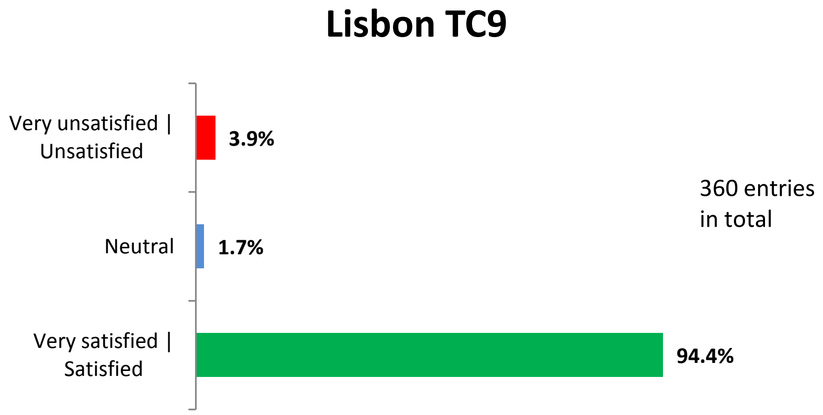


Figure 107 *TC9 Lisbon airport - Traveller satisfaction survey results*

6.5.2.2 Schipho

In Schiphol, only

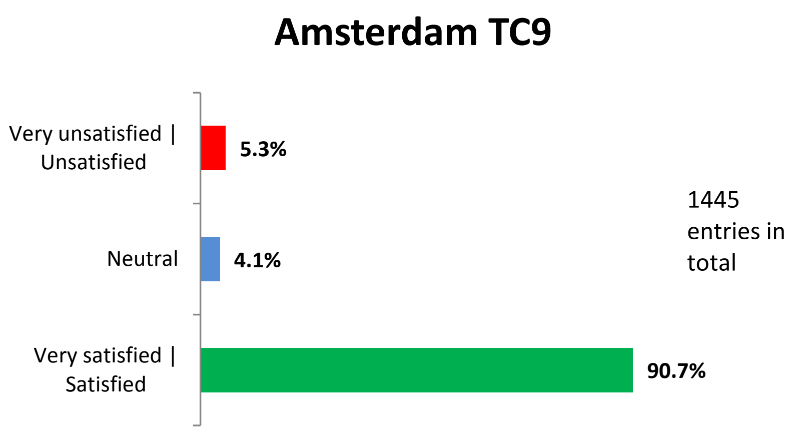


Figure 108 *TC9 Schiphol airport - Traveller satisfaction survey results*

6.6 Feasibility of extending the use of ABC gates at exit to TCNs

[Conclusion section to be added in Final Report]

7. Kiosk

7.1 Introduction

In recent years, self-service kiosks have been appearing at border crossing points around the world as an accelerator of the border clearance process. They are either used in conjunction with ABC-gate or travellers can find them before arriving at a manual booth. The main use cases that have been investigated are the following:

1. **Capturing data** from the passport immediately before the border crossing point;
2. **Verification** of the biometrics of the traveller and data in the passport;
3. **Enrolment** of biometrics.

The configurations of the solutions including self-service kiosks may vary greatly depending on different aspects, such as operational needs or conditions at the BCP. The specific technology deployed and its set-up can deeply impact the success of the implementation of a kiosk solution and the benefits that can be achieved. The expected benefits are:

- Higher throughput of passengers per booth, as each traveller spends less time with a border guard;
- Shorter queues;
- More efficient use of the existing space at the BCP;
- Reduced waiting time for travellers, resulting in potentially improved satisfaction.

7.1.1 Objective

The objectives of this chapter are to evaluate the usefulness, usability and security of using self-service kiosks for passport reading and checking or enrolling biometrics to reduce the border officer workload. The details of the objectives are to be found in the questions defined for TC10 and TC11, with the latter focusing especially on the use of kiosks at land borders.

The possibility of TCNs using kiosks at different border types has been assessed using the following metrics and structure:

1. **Operational and technological aspects**
    a. Quality
        - Are the enrolled biometrics of lower quality and which measures can help to prevent this?

    b. Duration
        1. How long on average does it take a traveller to go through border control from the moment s/he leaves the queue, uses the kiosk and then faces the border guard for each of the three variants mentioned in section 7.1 of this chapter (a. capturing data from the passport, b. performing biometric verification and c. enrolling biometrics) as compared to the manual control?

    c. Security aspects
        - How can the risk of travellers switching documents and spoofing biometric verification/enrolment be addressed?

2. **Human factors**

   a. Perceived benefits by border guards.

      - Do border guards perceive a benefit for each variant of the TCN preparing the border clearance? Benefits should relate in particular to workload.

   b. Perceived benefits by TCNs.

      - Do travellers perceive a benefit in using self-service kiosks for each of the three variants?

3. **Various constraints**

   a. Which environmental conditions influence the successful use of self-service kiosks under each of the three variants?

4. **Feasibility**

   a. For which type of large border crossings is the self-service kiosk suitable? Which border control operations can be performed/prepared by the traveller, according to the three main variants described previously?

The focus of the analysis is on kiosks used at entry. At exit the checks are less extensive and automation could be achieved through the use of ABC gates as discussed in chapter 6. Moreover, only kiosks coupled to manual booths, as opposed to kiosks that are part of an ABC- gate set-up, are included in the scope of the testing and research[90].

7.1.2 Kiosk workflows

This section defines the future potential usage of kiosks related to the business needs and border crossing processes. The options for use of biometrics related to the EES have been included in the process description without making any restrictions as regards future choices.

Possible functionalities that may be performed by a kiosk:

- Scanner for e-MRTD and MRTD documents;
- Chip reader for e-MRTD;
- Biometric enrolment/verification:
  - Reader for enrolling fingerprints (1-4 FP reader, 4 FP installed for supporting the Pilot);
  - Camera for facial image;
  - Iris (if retained as biometric modality).
- Bearer verification: Software for the verification of live FI against FI on the chip;
- Application for answering the questions TCNs are usually asked at entry.

[Process flow chart to be added in Final Report]

[90] In accordance with the Terms of Reference of the Smart Borders Pilot project.

7.2 Methodology

7.2.1 Use of Pilot results

Operational tests have been set up at the following four BCPs:

Border type	BCPs	Integrated/Not Integrated	Choice of biometrics
Air	Lisbon (PT)[91] *[test completed]*	**No**	**8FPs and FI**
	Madrid (ES)[92] *[test started]*	**Yes**[93]	**4FPs and FI**
Sea	Helsinki (FI)[94] *[test started]*	**No**	**8FPs and FI**
Land	Sillamäe (EE)[95] *[test not started]*	**No**	**8FPs and FI**

While operational results are the prime source of information, the following constraints made it necessary to complement them with consultations with MS experts and Frontex:

- **Limited possibility of integration:** the complexity of the integration, together with the tight timeline of the Pilot and strict data protection requirements, did not allow the kiosks to be integrated with border management systems and border control processes in most of the test instances;
- **Testing with stand-alone kiosks:** when not integrated, kiosks have been set up in the operational live environment with no connection to the real border management IT systems and not as part of the border control process. This limited the possibility to completely test functional systems and to collect data on the duration of the border crossing in comparison with a standard border clearance process at a manual booth (end-to-end measurements);
- **Limited possibility to test security:** it was not possible to perform comprehensive security tests to assess the ideal level of security, as it would have required the installation of several kiosks and a simulated use of the kiosk by impostors[96].

The illustrations below show the Pilot test configuration for the kiosk in the two scenarios: integrated kiosks and non-integrated kiosks.

[91] Further details on the test set up in ....

[92] Further details on the test set up in ....

[93] With the exception of VIS consultation, which does not take place at the kiosk during the tests.

[94] Further details on the test set up in ....

[95] Further details on the test set up in ....

[96] The term "impostors" is to be understood as persons actively attacking or misusing a biometric system, thereby trying to deceive the enrolment process.

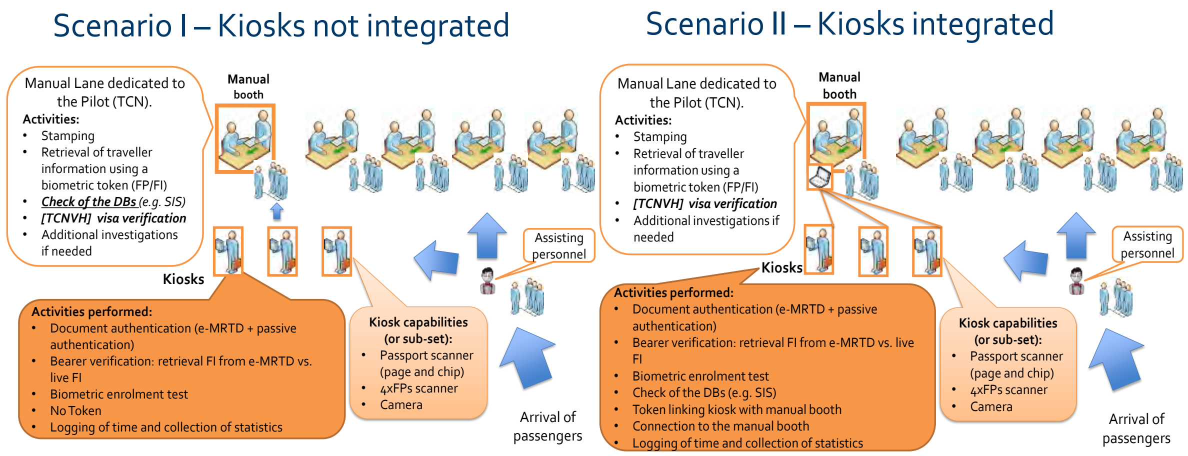

Scenario I – Kiosks not integrated
Manual Lane dedicated to the Pilot (TCN).
Activities:
• Stamping
• Retrieval of traveller information using a biometric token (FP/FI)
• Check of the DBs (e.g. SIS)
• [TCNVH] visa verification
• Additional investigations if needed
Manual booth
Kiosks
Activities performed:
• Document authentication (e-MRTD + passive authentication)
• Bearer verification: retrieval FI from e-MRTD vs. live FI
• Biometric enrolment test
• No Token
• Logging of time and collection of statistics
Kiosk capabilities (or sub-set):
• Passport scanner (page and chip)
• 4xFPs scanner
• Camera
Assisting personnel
Arrival of passengers
Scenario II – Kiosks integrated
Manual Lane dedicated to the Pilot (TCN).
Activities:
• Stamping
• Retrieval of traveller information using a biometric token (FP/FI)
• [TCNVH] visa verification
• Additional investigations if needed
Manual booth
Kiosks
Activities performed:
• Document authentication (e-MRTD + passive authentication)
• Bearer verification: retrieval FI from e-MRTD vs. live FI
• Biometric enrolment test
• Check of the DBs (e.g. SIS)
• Token linking kiosk with manual booth
• Connection to the manual booth
• Logging of time and collection of statistics
Kiosk capabilities (or sub-set):
• Passport scanner (page and chip)
• 4xFPs scanner
• Camera
Assisting personnel
Arrival of passengers

Figure 109 *Possible workflow with integrated and not integrated kiosks*

7.2.2 Configuration per BCP

Table 27 *TC10 Lisbon airport – TC configuration*

Duration of the test	3 weeks (from the 14.05.2015 to the 03.06.2015)
Timetable of the tests	Monday to Friday – 7:00 to 15:30
Layout	Kiosk in the arrival area plus dedicated Pilot lane in a manual booth
Sample size achieved	1455[97]
Technical integration	Not integrated
Integration within the regular border crossing process	Not integrated
Equipment type	Kiosk equipped with passport scanner, camera (FI) and 4FPs scanner
Enrolment/Verification Threshold	FI: Threshold based on verification matching score: 40[98] (vendor specific index – linear scale from 1 to 100) FP: NFIQ (2 for index, middle, ring fingers and 3 for little finger)
Traveller's survey	Survey on a tablet after the test
Test personnel	Shifts of 2-3 border guards: 1 border guard in the booth doing stamping and the normal border clearance procedure, 1-2 border guards recruiting volunteers and providing assistance if necessary.

[97] After data cleaning

[98] Expected FAR and FRR ≈1%

7.2.3 Sample characteristics

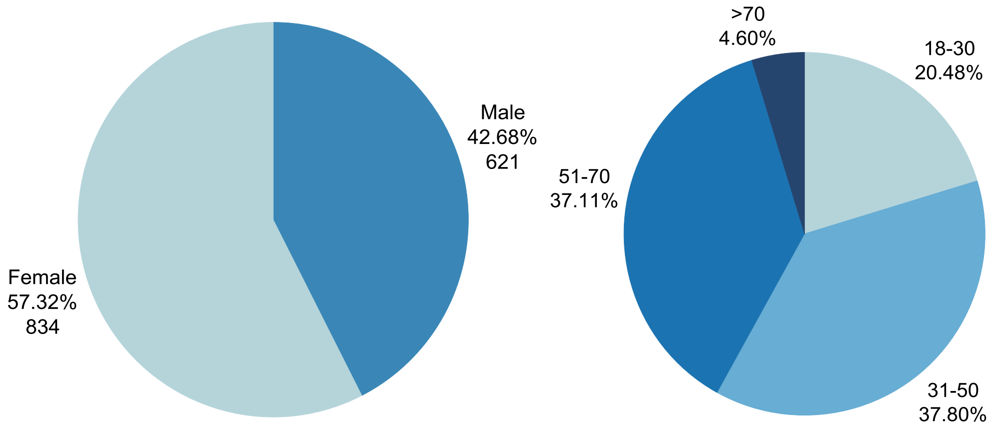


__Figure 110__ TC10 Lisbon airport **-** *Sample characteristics per gender and age*

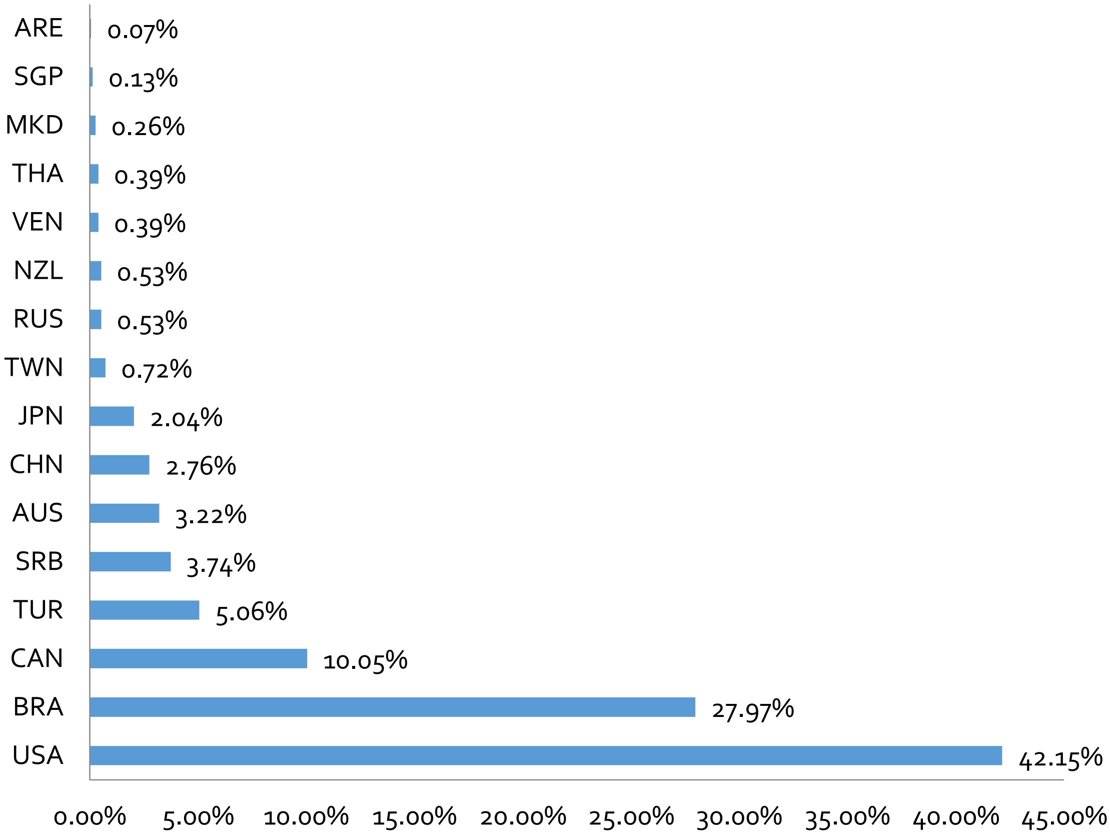


__Figure 111__ TC10 Lisbon airport - Sample characteristics per nationality

7.3 Technical and operational questions

Travellers often needed guidance for the capture and enrolment of biometrics: for fingerprints and for the correct positioning required to capture the facial image and iris pattern.

Observations from the field highlighted that the kiosk’s user-friendliness and ergonomics play an important role in reducing the need for guidance from border guards or civil assistance.

[Other observations from the field will be added as tests progress]

7.3.1 Quality aspects

Capturing a live photo and/or enrolling fingerprints, as a self-service function, could be difficult for a traveller not accustomed to this type of exercise. This section will try to gauge the difference in quality between the assisted process at the manual booth and self-enrolment at the kiosk.

A low quality of capture of the biometrics would have a negative impact on the feasibility of the kiosk for the purpose of self enrolment.

7.3.1.1 FP quality

7.3.1.1.1 Lisbon

At the kiosk, travellers were asked to enrol 8 FPs, using a 4FPs scanner. Enrolment was witnessed by a border guard located near the kiosk and ready to assist travellers if needed. The system would allow up to five attempts to enrol FP at the set NFIQ threshold[99]. The graph below shows that it was possible to achieve the set thresholds in 60 to 80% of the cases depending on the fingers.

[Comparison of FP enrolment at manual booth vs. self-enrolment to be added]

[Data cleaning still in progress – data might be subject to changes]

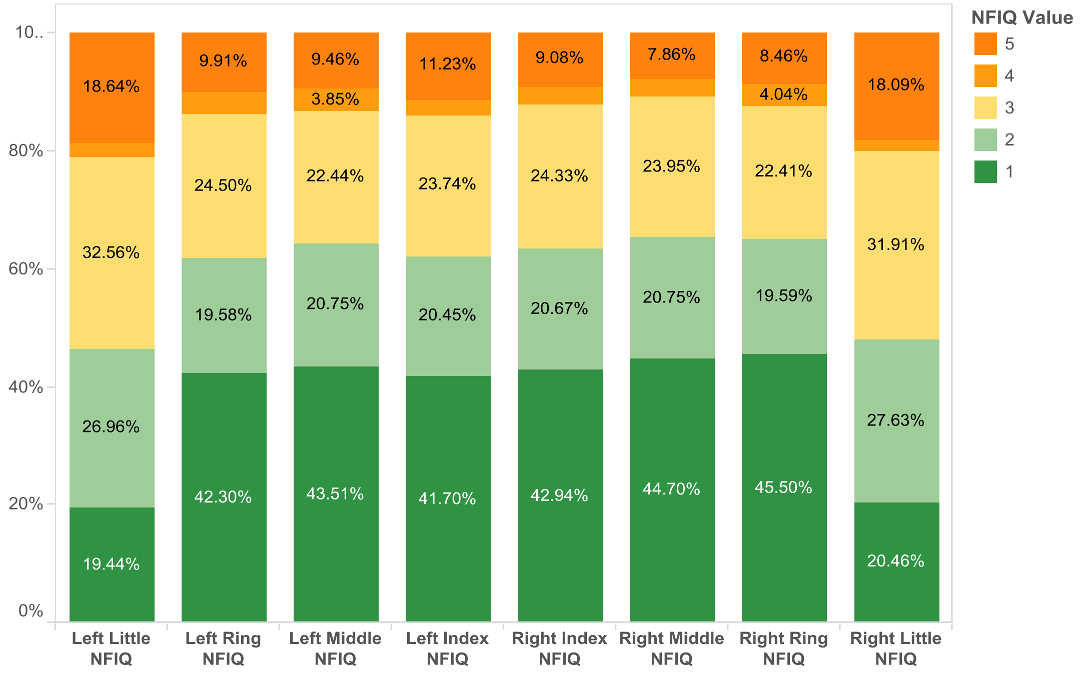


Figure 112 *TC10 Lisbon aiport - Distribution NFIQ scores per finger*

[99] Index, middle and ring NFIQ threshold of 2 and of 3 for the little finger.

7.3.1.2 FI quality

7.3.1.2.1 Lisbon

[Comparison of FI enrolment at manual booth vs. self-enrolment]

Live facial image quality score

The graph below shows the distribution of the quality achieved for the capture of the live facial image at the kiosk. The scoring is based on a proprietary quality index which ranges from 1 to 100. The results obtained show that it was possible to achieve good quality on the picture, with the majority of the sample, -85%-, scoring between 70 and 80.

[Data cleaning still in progress – data might be subject to changes]

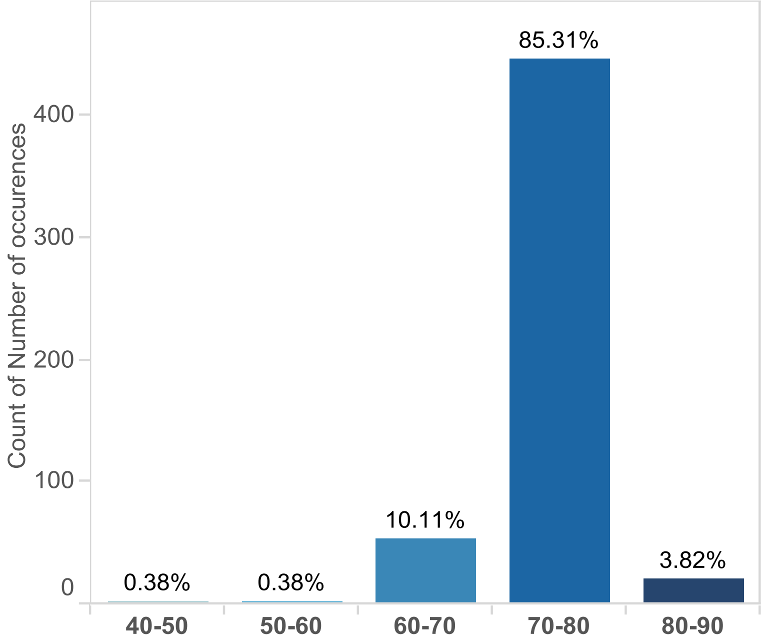


***Figure 113** TC10 Lisbon airport - Live facial image quality*

7.3.2 Duration

Throughout the tests the time spent at the kiosk was recorded for each traveller, as well as the durations of each individual step.

In addition, where the kiosk was integrated, the time at the manual booth was also captured in order to measure the end-to-end duration of the process and enable the comparison with the current process at the manual booth.

The duration of the end-to-end process only gives the service time for the check performed and not the actual negative or positive impact on traveller throughput for a given BCP. The throughput also depends on the number of kiosks set up and the combination of that number with the number of manual gates available.

This section will also analyse the durations of individual steps, such as the FPs enrolment, thus proving a higher level of granularity on what makes up the overall time spent at the kiosk. These individual durations are one of the elements to establish the feasibility of the different use cases for the kiosk of the self-enrolment of biometrics (FPs and FI).

7.3.2.1 Overall time at the kiosk

[To be completed for Final Report - Comparison of FP enrolment at a manual booth vs. self-enrolment]

[The time at the kiosk is time subtracted from the waiting time of the travellers. A number of kiosks can be deployed working in parallel, increasing the throughput by saving time at the manual booths.]

7.3.2.1.1 Lisbon

The graph below presents the distribution of the time spent by travellers at the kiosk. Travellers has spent

- Less than 110 seconds in 56% of cases;
- Less than 170 seconds in 88% of cases;
- More than 170 seconds in 12% of cases.

The median of the recorded values was 102 seconds. This time includes the time to enrol 8 FPs and the capture of the live facial image to perform the bearer verification.

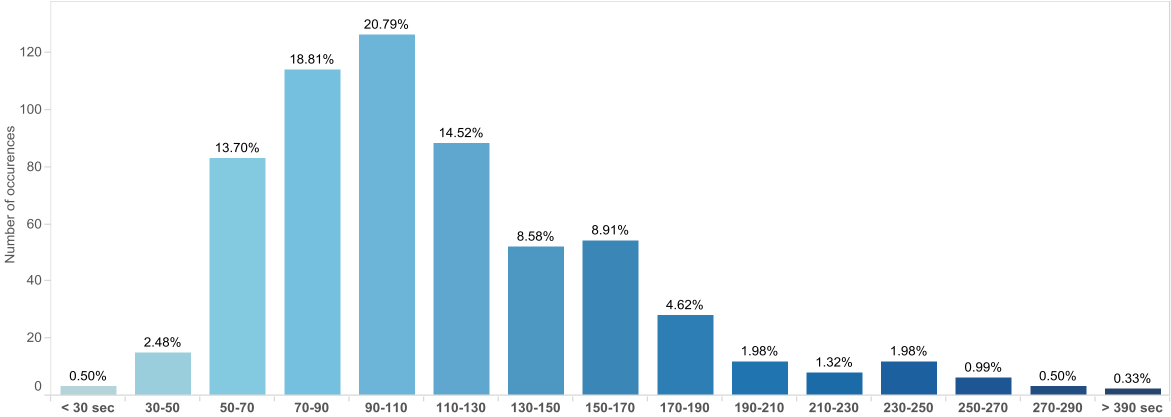


***Figure 114** TC10 Lisbon airport- Distribution durations at the kiosk*

7.3.2.2 Enrolment time for FPs

[Comparison enrolment FP manual booth vs. self-enrolment]

This section presents the results for the duration of the FPs enrolment at the kiosks. The self-enrolment of FPs clearly presents several challenges in terms of security, user friendliness and overall feasibility, however it is also one of most time consuming steps that could have to be performed at the manual booth and therefore also one of the main area of potential gain.

The capture of FPs for verification would be most likely shorter as lower quality thresholds could be envisioned for the verification which would not be acceptable in case of enrolment.

7.3.2.2.1 Lisbon

[Data cleaning still in progress – data might be subject to changes for Final Report]

The graph below presents the distribution of the time spent by travellers at the kiosk to enrol 8 FPs . Travellers has spent

- Less than 40 seconds in 60% of cases;
- Less than 60 seconds in 84% of cases;
- More than 60 seconds in 16% of cases.

The median of the recorded values was 35 seconds.

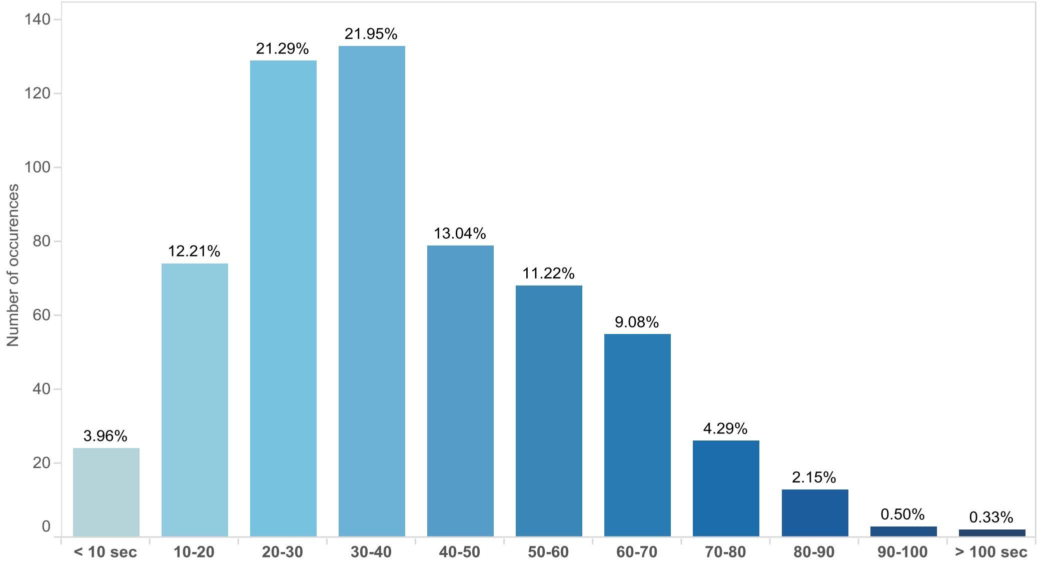


Figure 115 *TC10 Lisbon airport - 8 FPs enrolment time for TC10*

7.3.2.3 Time required for live FI capture and verification

[Comparison enrolment FI manual booth vs. self-enrolment for Final Report]

This section presents the results for the duration of the capture of the live FI at the kiosks and of its verification against the picture extracted from the e-MRTD. Such steps are necessary to perform the bearer verification.

7.3.2.3.1 Lisbon

Live image capture

[Data cleaning still in progress – data might be subject to changes for Final Report]

The graph below presents the distribution of the time needed to capture a live facial image of traveller, until the image reaches the threshold set on a matching score[100]. Travellers has spent

[100] The matching score is based on a vendor specific index.

- Less than 14 seconds in 57% of cases;
- Less than 15 seconds in 89% of cases;
- More than 15 seconds in 11% of cases.

The median of the recorded values was 21 seconds.

These results seem to be in line with what was recorded in the case of ABC gates.

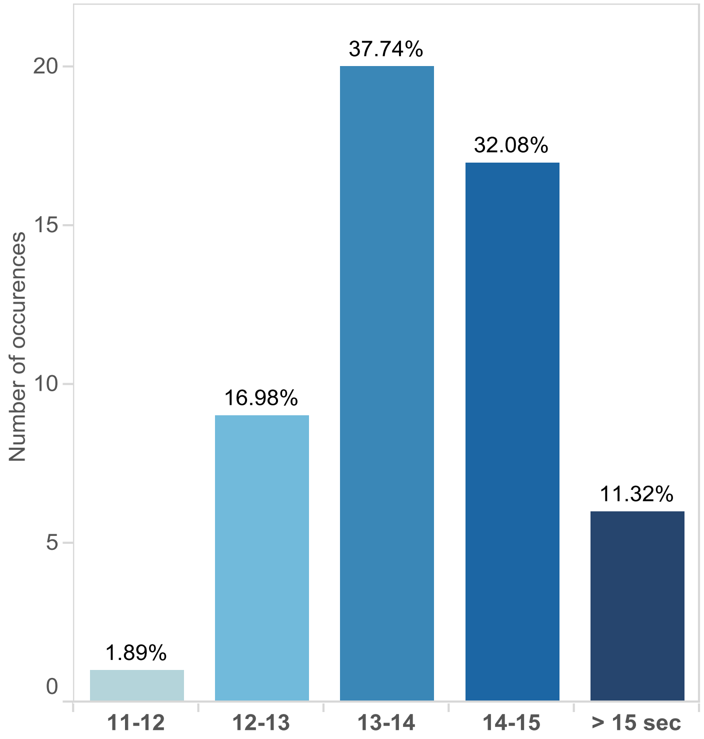


Figure 116 *TC10 Lisbon airport - Distribution live image capture time*

7.3.3 Security aspects

One of the key concerns linked to the deployment of kiosks is the required level of supervision. The need for supervision depends on the type of activities performed at the kiosk and in particular on whether biometrics are enrolled at the kiosk.

The main security risks are:

- Spoofing of biometrics (e.g. fingerprints)
- Impostors: use of another traveller's document to enrol biometrics or to cross the border
- […]

7.3.4 Risk mitigation measures

The following mitigations could further increase security:

Supervision

- An assistant or a border guard could supervise one or several kiosks that are not placed close to the manual gates.

  [...]

Demarcation and layout

- Placing and demarcation of the kiosk area are important aspects that influence the necessary supervision. A clearly demarcated area, not allowing more than one person to surround the kiosk, would make it easier to spot people trying to switch identities.

Video surveillance

- Video surveillance cameras can detect if more than one person is using the kiosk, which might indicate a spoofing attempt. Moreover, cameras can be used to allow remote surveillance of the location of the kiosks and may work as a deterrent against spoofing attempts.

Choice of the token

- The choice of the token can help reducing the risk of impostors or swap of identities. In fact if the biometrics enrolled are the same type as the one used as a token, this would mean that a given traveller would have to perform a second capture at the manual booth. For instance if a single FP was to be used a token, the traveller's FP would have to be captured again at the manual booth , in front of a border guard, in order to complete the process initiated at the kiosk. The FP in this case would be verified against the FP previously self-enrolled at the kiosk.

[....]

[Factors impacting the need for supervision – summary table to be added in Final Report]

7.4 Users' feedback

7.4.1 Border guards' feedback

7.4.1.1 Lisbon

11 border guards participated in and replied to the survey from Lisbon Airport**.** The **total number of replies received was of 29**[101].

The following dashboard presents a summary of replies[102].

Overall feedback[103] ★ ★ ★

Border Guard		Traveller
79% felt more confident with the equipment	90% rate the usability of the equipment as good	84% of replies indicated that travellers were mostly enthusiastic[104]

[101] They reported on a weekly basis over 3 weeks. 4 questionnaires are missing because of holidays.

[102] Percentages are calculated per question and are based on the number of replies given. In some cases, BGs have given more than one reply to one question.

[103] Rating: 3 * = good / 2* = neutral / 1* = weak.

[104] This is aligned with travellers' survey feedback showing 95.3% of satisfied or very satisfied answers for TC 10.

Potential improvement points

Border Guard		Traveller
Replies indicate that a movie showing how to use the kiosk would be useful	8% of replies indicate that the equipment could be more ergonomic	62% of replies indicate that more guidance to travellers could improve the process

Potential show-stoppers

Traveller	
Language 30%	Hardware problem 30%
19% of replies indicate that FP enrolment is difficult	Signal-system problem 9%
	Difficulty to use 4%

Observations and preliminary conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- **Overall, experience with passengers was positive and some points for improvement were mentioned**:
  - Technology (finger prints / iris/ facial recognition) is useful in case of doubt;
  - When FI verification is successful, the ticket should be printed automatically - currently necessary to press the next button on the screen;
  - More accurate instructions for travellers would ease the process.

- **Negative aspects:**
  - No added value in terms of security for kiosk;
  - Increasing the time spent per passenger as they were not able to use it autonomously;
  - Enrolment of fingerprints is difficult, especially for e.g. older travellers or travellers with scars on their fingers (as explained in chapter 3);
  - Not enough guidance to passengers putting the passport in the fingerprint recognition area instead of the passport reader.
  - Kiosk is sensitive to luminosity and should be placed on the way to the border crossing point. (as explained in section 7.5).

7.4.2 Travellers' feedback

7.4.2.1 Lisbon

The results collected in Lisbon and summarised in the chart below show that travellers responded overwhelmingly positively. Less than three percent of travellers were dissatisfied.

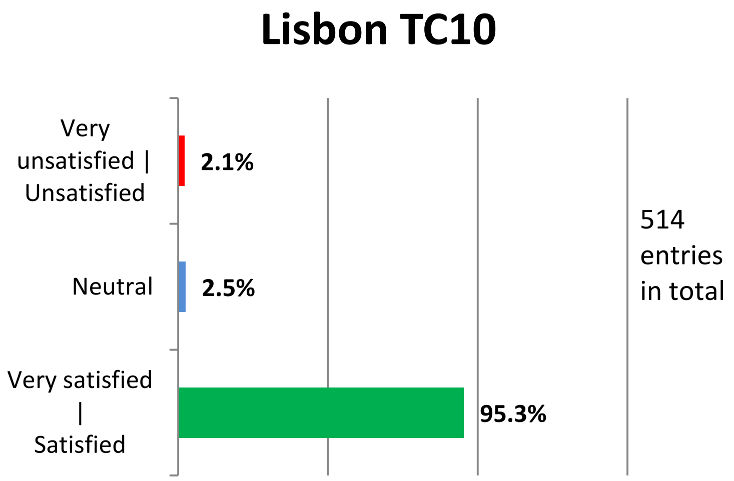


Figure 117 *TC10 Lisbon airport -Traveller satisfaction survey results*

7.5 Constraints

7.5.1 Environmental conditions

Environmental conditions play an important role in how successful technical devices are in the border control process. It is assumed that kiosks are used in indoor environments, which means that weather conditions should not be relevant.

Light conditions for photos and for capturing fingerprints are a valid factor when looking at the efficiency and feasibility of using self-service kiosks. The kiosks themselves normally have a built-in light for capturing an adequate live photo of the travellers. Too much external light or light that creates shadows could however be a problem for the performance of the camera and fingerprint readers at the kiosk.

Feedback from several border guards at Lisbon Airport indicates that there were several lightning problems, both for face and iris enrolment (e.g. passengers had to be asked to move to get more even lightning and iris/face capture failed seemingly due to lightning problems).

7.6 Feasibility

[Chapter to be completed for Final report]

8. Fallback scenario

8.1 Introduction

This chapter presents desk research related to managing situations where the EES is unavailable. The objective of the EES provides the means for abolishing stamping of passports thus speeding up border check procedures and providing information that could be used to prevent and fight terrorism and illegal migration. In order to do so, the EES must record all entries and exits of third country nationals at the Schengen Area external borders. In principle, no entry or exit should be possible without being recorded in the EES.

For causes which can be related to possible infrastructure outage either at national, communication or central layer, the EES could not be available to provide the services necessary to fulfil the abovementioned objective. In such cases there is a need to find solutions that mitigate the consequences of the unavailability: in this document, they are called "fall-back solutions". The described fallback solutions aim to handle unavailability of the EES at border locations and limit possible consequences at subsequent border crossings.

8.1.1 Objective

The desk research aims to present potential solutions and procedures for managing cases of EES unavailability and the possible consequences of such cases.

The desk research focuses on EES unavailability, **regardless of the specific individual cause of that deficiency** and without addressing generic border management issues and also without covering the complete border control process.

8.1.2 Attention points

Unavailability of the RTP is not explicitly mentioned in this document. The general principle for RTP travellers would be that they enjoy the RTP's benefits at the BCPs where and when it is available. In other cases the RTP traveller would simply need to use the normal process at a manual gate.

Business continuity planning elements are presented as a means of assessing risks and putting the likeliness of EES unavailability into perspective. This must be taken into account when looking at the proposed fall-back solutions.

8.2 Methodology

The potential solutions in this desk research are based on:

- Situations when a fall-back solution is needed, as identified in the Technical Study on Smart Borders published by European Commission in October 2014;
- Feedback from consultations with appointed experts from Member States, from the Study on Smart Borders and from eu-LISA's experiences with the existing mission-critical large-scale IT systems operated under its responsibility.

It is based on the following **assumptions:**

- The EES would provide services and function as described in the Technical Study on Smart Borders taking into account the options presented in the Study. These functions relate to searches in the EES, verification, identification and registrations of data in the EES;
- Although availability requirements have not been defined for the EES, it is assumed that the requirements for searches and registrations would be comparable with, or more stringent than, those

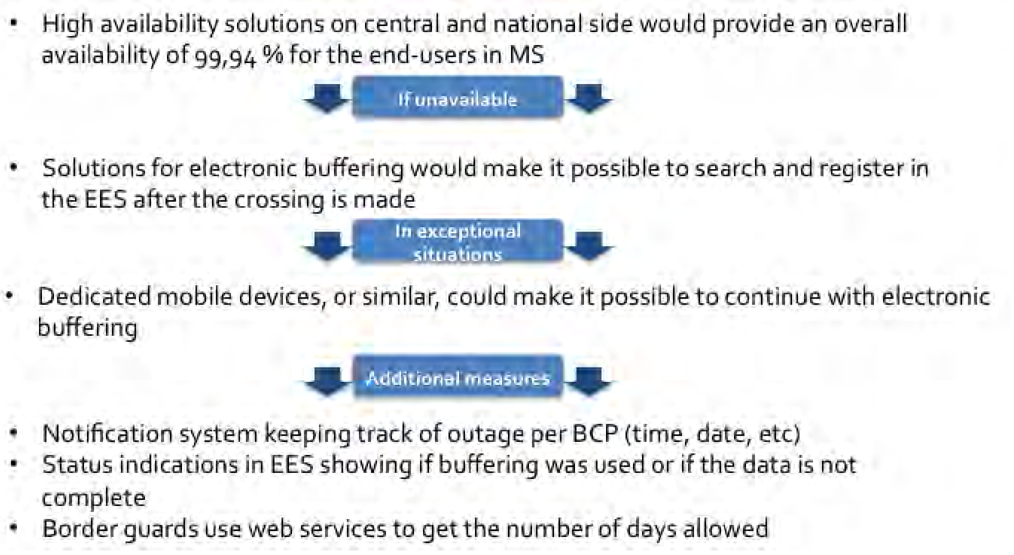
for comparable systems e.g. SIS II[105] and VIS[106];

- Unavailability of the EES would have a negative impact on the traveller. This is not the case if the SIS II or VIS is unavailable, which needs to be taken into account;
- The policy for the EES is assumed to include that all entries and exits must be recorded with a 100 % coverage. Missing entries or exits will therefore be treated as exceptions in this research;
- The reasons why the EES would be unavailable are not explored in this desk research, unless the reason has a direct impact as regards how to handle the unavailability;
- The desk research does not address partial unavailability or response time problems. The solutions presented are there to handle the cases when it is not possible to use the EES at all.

The approach of the desk research is as follows:

1. To firstly look at the measures for achieving high resilience of the EES at a central and national level, including the main elements of a business continuity planning process.
2. Secondly to look at measures that can mitigate the consequences (*i.e.* electronic buffering and certain supporting solutions) of EES unavailability
3. Thirdly to look at solutions in exceptional circumstances where no mitigation measures are available.

The approach is presented below from a conceptual standpoint:



- High availability solutions on central and national side would provide an overall availability of 99,94 % for the end-users in MS

If unavailable

- Solutions for electronic buffering would make it possible to search and register in the EES after the crossing is made

In exceptional situations

- Dedicated mobile devices, or similar, could make it possible to continue with electronic buffering

Additional measures

- Notification system keeping track of outage per BCP (time, date, etc)
- Status indications in EES showing if buffering was used or if the data is not complete
- Border guards use web services to get the number of days allowed

Figure 118 *Conceptual approach*

The overall availability mentioned in the figure above assumes that the business continuity planning presented in the next section is implemented.

[105] Commission decision 2007/171 states: *The CS-SIS and the LNI and BLNI must be able to deliver an availability of 99.99 % over a 28-day rolling period excluding the network availability. The availability of the Communication Infrastructure must be 99.99 %.*

[106] The eu-LISA report to the EP in 2014 states: "*VIS was designed to offer a high level of reliability, implying full system availability, robustness and data integrity; as such, the system should be fully available to all end users 99.99% of the time.*"

8.3 Business continuity planning

The implementation, and related costs, of fall-back solutions should be balanced against the likeliness and impact of the EES not being available. To assess this balance, further elements of a hypothetical business continuity plan are outlined below. The outline is based on a conceptual view of the end-to-end solutions for the EES, simplified as an architecture consisting of six levels.

6. End-user environment (e.g. workstations, mobile devices)

5. National network

4. National systems used in the context of border management

3. National Uniform Interface (NUI)

2. Central network

1. Central EES

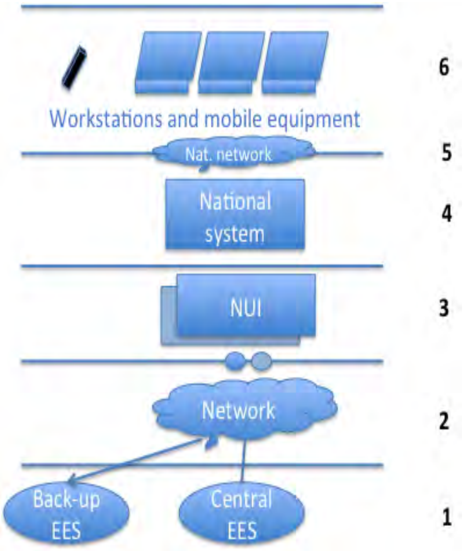


***Figure 119** End-to-end solutions for the EES*

8.3.1 Architectural requirements

Central EES and central network (level 1 – 2)

The central EES's availability must be high to ensure that its objectives are reached. It can be assumed that the central EES, including the central network, would have a Service Level Agreement (SLA) corresponding to an availability of 99.99 % on a rolling 28-day period. To reach such a level, the following main elements are needed:

- A central back-up system, mirroring the EES, preferably with an "active-active" concept;
- High availability, overcapacity and redundant solutions at a network level, including back-up access points for Member States connections to the network;
- An infrastructure that includes solutions for uninterrupted power supply (UPS) at a central and network level, in line with the SLA;
- Procedures and routines for supervising, managing and taking countermeasure, promptly, when blocking incidents occur;
- Fully integrated and enforced test and release management policy including the possibility to simulate the process in a near operational technical environment.

NUI (level 3)

The NUI would basically function as an intermediary between national systems and the central system, providing the services for accessing the EES and taking care of the necessary buffering, etc. It should have at least the same level of SLA as the central EES and would therefore require basically the same elements of resilience to reach this level, tailored to the size and throughput of the NUI.

National systems and national networks (level 4-5)

The use of the term "national systems" is quite widespread. In this context it includes all the national systems that contain the business logic for serving the border checks, excluding the presentation layer to end-users. These systems fall fully within the remit of the Member States. To achieve the full objectives of the EES it has to be assumed that these systems, and their related infrastructure, would need to be designed with the same SLA as the central EES. The same features designed to provide high availability as described for the central EES should be addressed (e.g. UPS, redundancy, procedures, advanced testing of releases and monitoring).

End-user environment (level 6)

The end-user environments are also assumed to have the same level of SLA as the central EES. The IT architecture is different for each Member State but it can be assumed that the main elements related to the availability of end-user environments are to have uninterrupted power supply and to perform exhaustive quality control of new/changed applications.

8.3.2 Overall availability of the EES

The different technical levels above could be divided into six levels, when counting the central and national networks as separate components in the business continuity plan. **The assumption for the business continuity plan presented is that each level would have the same service availability requirement (99.99%). Should this not be feasible to achieve then the proposed solutions for electronic buffering are still valid but the volumes to handle in the buffering would increase.**

In a worst-case scenario, when unavailability at all levels occurs in the same timeframe, this would mean a total availability of 99.94%, in a measured rolling 28 day period, at end-user level. In practice this means 26 minutes of potential unavailability for a given BCP.

It should be noted that in the potential period of unavailability it is only the EES searches unavailability that has a direct impact on border guard work. With the solutions for electronic buffering described in the next section, the EES search and Entry/Exit updates could be made after the person has left the border crossing point.

8.3.3 TCNVHs – specific conditions

When looking at solutions to mitigate EES unavailability, the difference in handling TCNVHs compared to TCNVEs must be considered. The need for enrolment of fingerprints at border should not concern TCNVHs and these travellers' credentials should be verified against the VIS, as is the case today, and not against the EES.

In other words, if the EES is unavailable, the inability to run a search in the EES is not as vital for checking a TCNVH as it is for checking a TCNVE and there is less data to be registered in the EES. Nevertheless, the creation of an entry/exit record is mandatory for TCNVHs, which must be considered in the business continuity plan.

The future architecture where the EES, RTP and also VIS, will be implemented is yet to be studied and decided on.

At present the VIS resides on a dedicated platform, with its own infrastructure and its own usage of the central network. The Technical Study outlines options where the EES and RTP are separate systems and also alternatives where they are part of a common architecture, including the current VIS functions.

The desk research addresses primarily the unavailability of the EES, though as regards TCNVH travellers the availability of the VIS needs to be taken into account. As long as the VIS can be accessed at end-user level these travellers can be verified. This would be possible even if the EES would not be available given that they would be separated in terms of architecture and infrastructure.

In the case where the EES and VIS share resources the unavailability of central resources would have a different impact and this would have to be taken into account in a business continuity planning.

8.4 Fall-back solutions

The measures that are outlined in the business continuity plan would enable the central EES and the functions of the EES at end-user level to reach a high level of availability. Where EES functions would be unavailable, however, there would need to be other solutions to maintain the data in the EES. This chapter looks at a number of potential solutions.

8.4.1 Electronic buffering

When the central levels (level 1 and 2) are unavailable, electronic/automated solutions could be used for capturing and buffering travellers' alphanumeric data and biometrics at a national level, which would be entered in the system later. It should therefore be possible to capture all alphanumeric and biometric data necessary for a full EES registration.

The buffering solution does not cover cases where the EES should have informed that a person is an over stayer. The border guard cannot provide the traveller with this information. A possible solution would be for the border guards to use the web services, proposed in the Smart Borders Study to check the number of days for a given person. If the web services are not possible to use, the problem could only be dealt with at subsequent crossings.

There is no way of determining whether it is the first time the traveller crosses the border, at entry. Data and biometrics for the individual file must therefore be acquired and buffered for every traveller.

The data buffered locally must be automatically flushed after the registration in the EES is acknowledged as complete.

Once the EES is again fully available to the end-users the search and registration could be made with a high degree of automation, meaning that the buffered data is used for automated searches and batch registrations with little intervention needed from the border guards. If the EES search shows that it is the first border crossing for a traveller, the individual file is created.

If the buffered data indicates a first-time crossing of a TCNVE the fingerprints buffered could be used for identification purposes (1:N[107]) in the EES. If it is found that the person appears in other individual EES files, this could possibly be signalled for later actions by looking at a method for "marking" the EES record (*i.e.* setting a status flag) in order to check the person with more attention at the subsequent crossing.

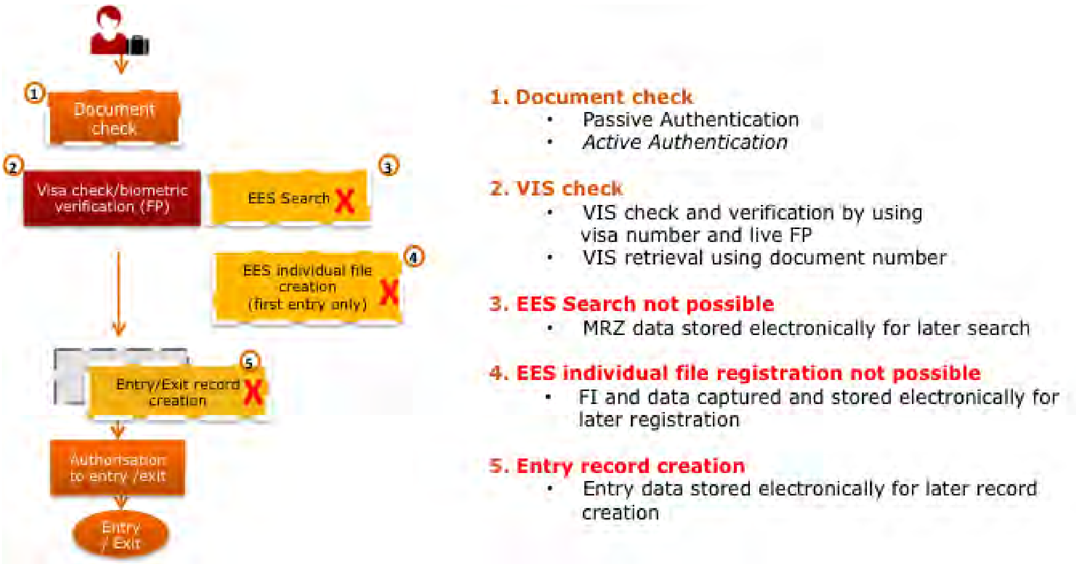
The value of identification (1:N) of a TCNVE in this scenario is somewhat doubtful since the person is not anymore present to answer any questions related to possible findings or problems when performing these checks.

[107] 1:N identification is proposed as an option in the Smart Borders Technical Study. The text as regards this option is only valid if it is retained in the final solution for the EES.

When using the buffered data and finding the person in the EES, and where the person is TCNVE, the biometrics (*i.e.* fingerprints or facial image) could be used to verify the person's identity. If the verification yields negative results this could possibly be handled by looking at a method for "marking" the EES record (*i.e.* setting a status flag) in order to check the person with more attention at the subsequent crossing.

8.4.1.1 Border control process

This section describes an excerpt of the border process related to a situation where EES functions are unavailable and where electronic buffering is used. The process described is on a logical level and does not take into account technical solutions not yet decided on. In the process below the VIS is therefore regarded as a separate source of information not impacted by the EES unavailability.


1
Document check
2
Visa check/biometric verification (FP)
3
EES Search X
4
EES individual file creation (first entry only) X
5
Entry/Exit record creation X
Authorisation to entry /exit
Entry / Exit

1. Document check
   - Passive Authentication
   - *Active Authentication*

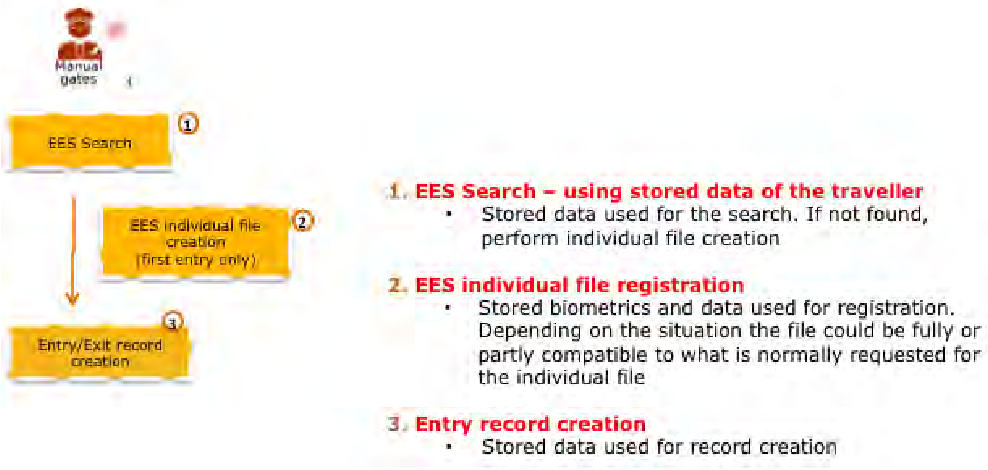
2. VIS check
   - VIS check and verification by using visa number and live FP
   - VIS retrieval using document number

3. EES Search not possible
   - MRZ data stored electronically for later search

4. EES individual file registration not possible
   - FI and data captured and stored electronically for later registration

5. Entry record creation
   - Entry data stored electronically for later record creation

Figure 120 *Process for border check at entry when the EES is not available – visa holders*

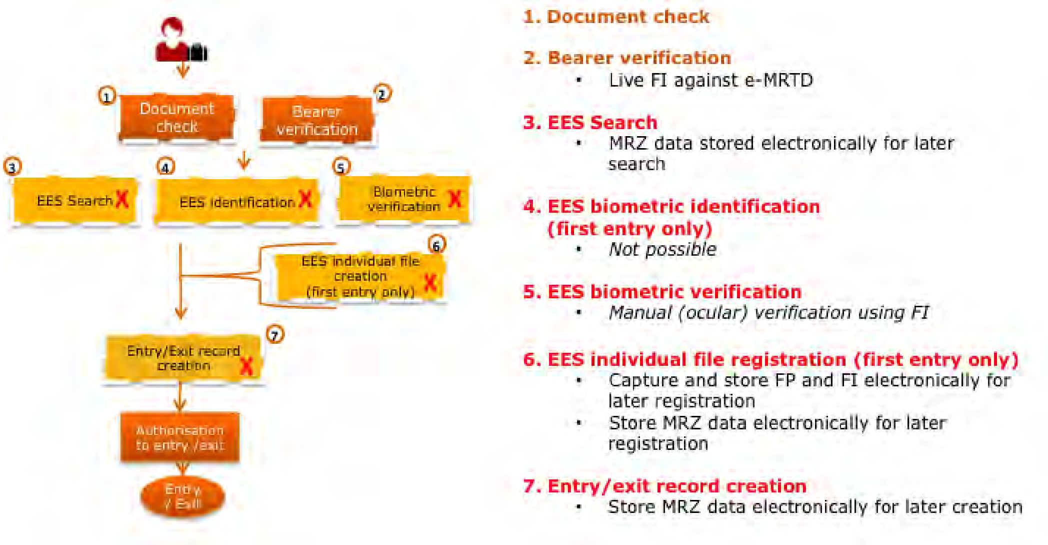

Manual gates
EES Search
1
EES individual file creation (first entry only)
2
Entry/Exit record creation
3

1. EES Search – using stored data of the traveller
   - Stored data used for the search. If not found, perform individual file creation

2. EES individual file registration
   - Stored biometrics and data used for registration. Depending on the situation the file could be fully or partly compatible to what is normally requested for the individual file

3. Entry record creation
   - Stored data used for record creation

Figure 121 *Search and registration of data and biometrics at entry – visa holders*



1. Document check

2. Bearer verification
    - Live FI against e-MRTD

3. EES Search
    - MRZ data stored electronically for later search

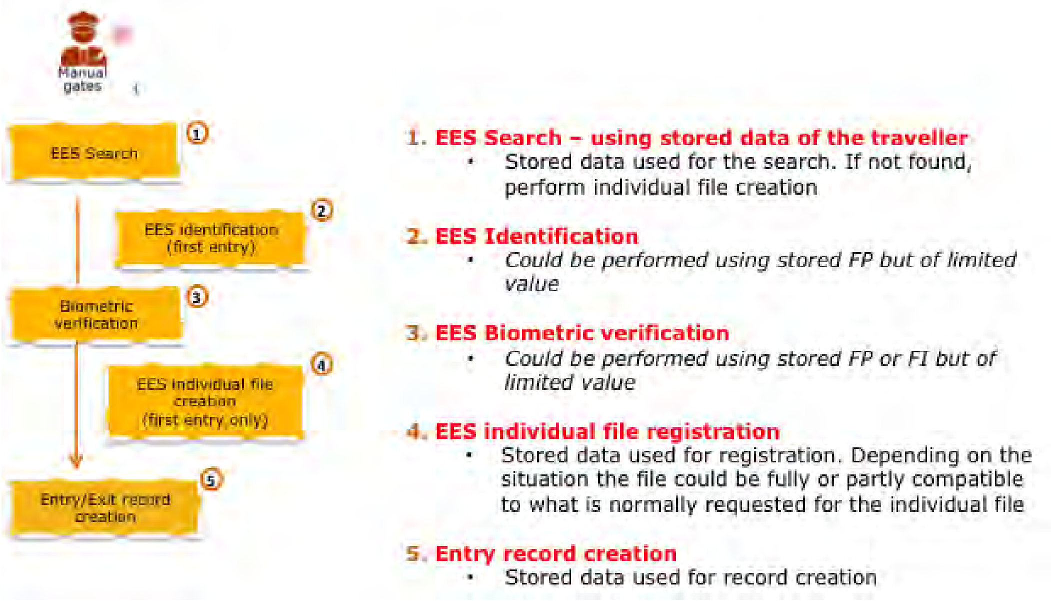
4. EES biometric identification (first entry only)
    - *Not possible*

5. EES biometric verification
    - *Manual (ocular) verification using FI*

6. EES individual file registration (first entry only)
    - Capture and store FP and FI electronically for later registration
    - Store MRZ data electronically for later registration

7. Entry/exit record creation
    - Store MRZ data electronically for later creation

Figure 122 *Process for border check at entry when the EES is not available – visa exempt*


Manual gates
1
EES Search
2
EES identification (first entry)
3
Biometric verification
4
EES individual file creation (first entry only)
5
Entry/Exit record creation

1. EES Search – using stored data of the traveller
    - Stored data used for the search. If not found, perform individual file creation

2. EES Identification
    - *Could be performed using stored FP but of limited value*

3. EES Biometric verification
    - *Could be performed using stored FP or FI but of limited value*

4. EES individual file registration
    - Stored data used for registration. Depending on the situation the file could be fully or partly compatible to what is normally requested for the individual file

5. Entry record creation
    - Stored data used for record creation

Figure 123 *Search and registration of data and biometrics at entry – visa exempt*

8.4.1.2 Technical and architectural aspects

The solutions for electronic buffering can be implemented on different levels on the national side, where the last resorts for buffering are workstations or mobile devices used by border guards. It is likely to assume that mobile devices are designed to cope with a shorter period of outage than workstations, the national system and/or the NUI.

Of the six levels of architecture presented in the business continuity plan, the upper three levels, on the national side, would all be targets for implementing solutions that can buffer data and biometrics. At each level, it should be possible to buffer data independently of the other levels.

Aspects to consider:

- National end-user applications, devices and systems would have to be adapted in order to cater for buffering and the lack of a search function against the EES;
- Asynchronous communication should be possible between the architectural levels in cases of outage when electronic buffering is used;
- The NUI should have functions for buffering and automated registration as well as functions for receiving buffered data from national components and carrying out the searches/registrations;
- Depending on the architecture in the Member State, it might or might not be possible to do electronic buffering in at workstations and/or on the mobile devices used. In those cases, it is proposed that the national systems are proposed to handle the necessary buffering. In the cases where buffering can be made in at workstations/on mobile devices, it would be an option not to have any functions for buffering in the national system;
- Buffered data must be secured for data protection reasons.

Buffering at the NUI level

The NUI could contain functions for storing data and biometrics when EES is not available and also functions for automated searches and registrations once the EES is available again. It is possible to make the automated registration cover all types of cases, thereby avoiding the need for manual intervention. Exceptions would be notified to the border guards (*i.e.* back-office functions of the BCP).

This solution would have the benefit of enabling border guards to continue to work more or less as normal, except that real-time searches cannot be performed at the time the person is checked. If the central EES or the central network is out, the national systems could in principle continue to function as normal.

As regards the technical challenges for performing the buffering, search and registration, the following factors should be considered:

- Concurrent updates of a travellers EES data from other end users (e.g. another NUI) are quite unlikely to occur since the update relates to the individual traveller crossing or just having crossed the border. The NUI function for creating EES records can be built on this assumption;
- EES data for a specific individual should not be dependent or related to data on other individuals in the EES. There should therefore be no need to implement a complex queuing and transaction-handling process to perform the registration;
- The registration function should not need to update existing data but rather add data in the EES, either a new EES individual file with an entry/exit record or only an entry/exit record. Corrections or updates of individual fields in existing files should not need to be included as a function;
- The NUI should be able to buffer and balance batch searches/updates in order to minimise the impact on the central system. The central system does however also need to be able to handle peaks, in relation to the buffering and batch searches/updates made by the NUI.

The above characteristics of the NUI are also valid if national systems, workstations or mobile devices have buffered data, while the NUI was not available, and need to send this data to the central EES via the NUI.

Buffering in national systems

If the NUI is not available or does not handle the abovementioned electronic buffering, the national systems in the Member States could be developed with the aim to cover the need for electronic buffering.

It would be quite complex, and virtually impossible, to centrally develop the function needed and implement this within the national systems. It could however be envisaged to develop common specifications for buffering at a national level that MS would use to develop their national systems. As part of the solution there should be corresponding functions of the NUI, to be used for "batch" searches and registration once the EES is available.

This kind of solution could be used as a complement to the buffering of the NUI thereby limiting the risk of not having electronic buffering available.

Buffering at workstations/on mobile devices

In certain cases, a local buffering of data and biometrics at the border guards' workstations and on their mobile devices could be a complementary means. Member States would, as in the case of buffering in national systems, implement these kinds of solutions, preferably through common specifications used by all Member States.

In the same way as for buffering in the national systems the NUI could contain functions for later "batch" searches and registration of data buffered at workstations/on mobile devices.

8.4.2 Alternative solutions for exceptional circumstances

The electronic buffering described in the previous section should cover in principle 100% of the cases when the EES is not available. In rare cases when the described electronic buffering is unavailable (*i.e.* buffering on level 3-6 is not possible) alternative solutions could be looked at.

The table below summarises the solutions looked at for handling buffering in exceptional circumstances. A scoring of – up to ++ is used to assess the solutions,++ being the most positive in relation to the column's heading.

Table 28: *Summary table – alternative solutions*

	Usefulness in exceptional circumstances	Basic functions	Maintenance	Cost efficiency	Security
Common mobile devices	+	+	-	--	-
Mobile app	+	+	-	-	-
USB for workstations	--	-	--	+	--
Alternative communication channel	-	++	--	-	+
Border procedure for completing EES registration (using physical stamp as evidence for the missing recording)	++	N/A	+	+	Neutral[108]
Border procedure for completing EES registration	++	N/A	++	++	Neutral[109]

[108] Making the registration in EES complete should have equal impact on risks as todays procedure for handling missing stamps

[109] Making the registration in EES complete should have equal impact on risks as todays procedure for handling missing stamps

Common mobile devices

An idea could be to set up and make mobile devices available to all BCPs or to BCPs that are seen as having high priority. These would be used only in the cases where the "normal" electronic buffering does not work, for instance if a power outage goes beyond what the UPS can handle, leaving end-user workstations without electricity.

Existing mobile devices already used by the Member State for regular checks could also be used to buffer data. These would however be integrated to the national infrastructure which could make them more vulnerable in cases of outage of EES. Still, this is also an alternative and should be part of a business continuity planning.

The mobile devices provided from the central level would include basic functions for capturing and storing alphanumeric data, and possibly also biometric data. As soon as the national infrastructure would be working again these devices could empty their buffered data, to be forwarded to the NUI via national systems and processed towards the central EES.

The basic functions would be centrally developed and uniform across the devices deployed.

In general, this idea was found worth pursuing further by the participants at the expert meeting on 19 May 2015, however, the experts also saw a number of issues that to be looked at and analysed further.

Comments from the Member States' experts and internal discussions at eu-LISA point to the following areas that need further investigation:

Basic functions of the devices

The basic functions would be the same as what the border guard normally uses for the EES, with some limitations. Search functions are not possible and the device would be offline when used for buffering. Capturing of data and biometrics for the individual file and for the recording of the entry/exit would be the core functions. An option put forward at the expert meeting would be to agree to only gathering and registering alphanumeric data, thereby reducing complexity and costs. The consequence of this agreement would be that in these cases that biometric data would not be registered in the individual file at entry and biometric verification of identity at exit is not possible.

Once it is possible again, the device would connect with the NUI via national systems and empty the buffered data. This would be treated by the NUI as any other buffered data coming from national systems.

Maintenance

The devices would have to be kept under central maintenance by eu-LISA, including normal activities such as release management, trouble shooting/incident management, regular function tests and correctional updates. Remote access to the devices would be needed, either through national networks or via separate communication channels.

Cost efficiency

Given a high availability of the central and national solutions as well as electronic buffering solutions in the case of EES unavailability, the use of the devices would be quite rare. It is likely to assume that they would stay untouched for long periods. The balance between the added value of the devices and the costs would have to be considered. For instance, only selected BCPs could be provided with the devices. A factor to consider would be that small BCPs (e.g. a small harbour) are more likely to encounter situations where the existing infrastructure is not providing buffering or EES access. On the other hand, the volumes handled at such small BCPs, in a period of outage, are most likely very small; as a result, they may not justify the need for mobile devices to be deployed there. Large BCPs do have the volumes that justify the need for mobile devices but they also have a much more resilient infrastructure, where mobile devices would only be needed in very rare cases. A risk of the rare use of these devices could be unfamiliarity with the devices when needed, causing user problems and leading to incomplete registration.

Security

National security rules and technical solutions must be taken into account when defining a solution that includes mobile devices deployed by an external entity, as seen from a national perspective. The problems of solving these are less complex when it comes to using the device for off-line buffering of data and biometrics. The challenges in this area relate to how to transmit the buffered data in the devices, via national systems, to the NUI, where national firewalls and other security solutions must be passed. Firewalls and other relevant components would normally have different configurations in each Member State and communication from the device must be compatible with all of them.

Mobile app

An alternative to the mobile devices could be to develop an "app" that would contain the basic functions needed for buffering data and electronics. The buffered data would have to be transmitted to national systems via secure communication and passed on to the NUI. This would mean that MS already have a mobile device available?

Issues to be further considered:

Basic functions of a proposed app

The basic functions would be the same as in the mobile device. The app would have to be compatible with the main mobile operating system available in the market (e.g. Android, iOS), downloaded via a secured website (or a public catalogue if security solutions exist for such a solution) and, like any other app, it would also need to be updated regularly.

Maintenance

The app would be centrally maintained, including normal activities such as release management, trouble shooting/incident management, regular function tests and correctional updates Specific procedures or solutions are needed to ensure that end users regularly update the app to the newest release and always before using the app for buffering.

Cost efficiency

Compared with mobile devices, the possible advantage of an app is that there are no extra costs if the app stays unused. Maintenance costs are therefore likely to be lower and there would be no need to prioritise the BCPs, which would be provided with them.

Security

National security rules and technical solutions must be taken into account when developing and using National security rules and technical solutions must be taken into account when developing and using an app for buffering. As is the case for mobile devices, the off-line buffering should not be a security issue but communication from the app to the NUI must be compliant with national security rules and solutions.

3G/4G/5G at workstations

An idea proposed at the expert meeting was to look at using USB, with mobile communication connection (3G or future versions), to store and communicate buffered data. This would work as a fall-back solution when workstations are available but the national systems are not.

Basic functions

Using the USB for buffering and communication of buffered data would entail either that all end-user workstations contain a specific centrally developed application only used for this purpose and these situations or that national end-user applications are made able to switch to interface with the USB instead of their normal communication route.

Maintenance

The USB would have to be developed and deployed centrally. A specific application to be used for this purpose would also have to be centrally developed and maintained by the central level. The problem in this case could be the mechanisms used in each Member State for including a new application at workstations and/or for updating them. The central functions for propagating the application would have to comply with all variants in this area used by Member States.

Cost efficiency

The USB as a solution would only work when the workstations are still functioning. It does therefore not cover the business needs in the same way as a mobile device or an app for mobile telephones would do. USBs would have to be deployed to all workstations at all BCPs, or to the ones that are selected due to defined priority rules, as for mobile devices. If a common application is used, it must be deployed to and maintained at all BCPs, or at the ones that have been given the USB. A central application would also have to be updated and tested in the cases where the workstation environment is changed at national level. If the national applications are to interface with the USB, these need to at all BCPs using the USB and maintained in accordance with central changes to EES data.

Security

National security rules and technical solutions must be taken into account when integrating solutions to the end-user workstations. This puts requirements on compliance both for the USB, its communication ability and a common application used for registration to the USB. Communication from the USB using 3G (or future versions) would also have to comply with national security rules, firewalls, etc. An alternative would be to use the USB only for buffering; in that case, the USB would have no external communication feature. The data would then have to be emptied to the workstations and forwarded as buffered data to the NUI.

Alternative communication channel

A solution already used in one Member State is to have the workstation and the concerned applications adapted so that they can use an alternative communication channel at times of outage of national systems or networks. This could mean, for instance, that buffered data would be sent directly from the workstation to the NUI without passing through the national systems and the "normal" national networks.

This solution would be an alternative that would not be developed centrally but would be for Member States to assess whether it would be of added value, hence why there is no detailed assessment in this document. The buffered data sent and communication to the NUI would have to comply with the specifications of the NUI's functions for the purpose of receiving buffered data.

Border procedure for completing EES registration

In accordance with the existing procedure in the Schengen Borders Code, there could be a procedure for amending/completing the EES registration for travellers arriving and having a missing entry or exit. When presenting it here as an alternative solution it would include the option to either keep the physical stamping or not. The purpose of the physical stamp would be to serve as additional evidence of the entry or exit that is missing. A trade off would be to accept, for the extremely limited number of cases this occur, that there would be less firm evidence on the date and place for the missing crossing.

Basic functions

This solution is built on the existing procedures of the Schengen Border Code and needs not specific technical solution to be implemented.

Maintenance

With stamping: The routines and equipment for the manual stamping would have to be kept and updated continuously.

Without stamping: No maintenance needed, the procedure would at any rate be included in normal training.

Cost efficiency

With stamping: Costs for keeping the stamping procedures, equipment, etc. would still remain. Compared to other alternative solutions the costs are however limited.

Without stamping: No costs for maintaining stamping and virtually no costs at all for this alternative, which makes it very competitive in relation to the other alternatives presented (as regards costs).

Security

With or without stamping there is no security impact related to border management systems or procedures.

8.4.3 Additional supporting solutions

Besides electronic buffering there are other solutions that could help provide relevant information when the EES is unavailable and giving end-users or travellers the information they need.

8.4.3.1 Notification system

Information on outages can be used for supporting border guard's decision making, when travellers appear without a complete EES registration and there is a need for proofing that this incompleteness occurred at a BCP and a time when there was an outage. It could also be useful data for statistical purposes. Therefore it could be an option to implement a notification system. This would involve Member States systems, where information on local outage should be sent to the central level and central EES functions could also detect outages not related to the central system itself.

8.4.3.2 Status indications in the EES

When the EES is updated using buffered data, or in other situations when normal routines are not followed, a status indication could be set in the EES. This would indicate, for example, the need for extended checks of the EES to ensure quality or the need to complement the EES file.

8.4.3.3 Web services for Border guards

Even with electronic buffering, the EES search will be unavailable. This means that the border guard would not be able to see whether the traveller has enough days left and the traveller could not be informed in this regard. A proposed mitigation for this would be that the border guards use, via internet, the web services that are intended to serve carriers and travellers with information on the number of days used of the authorised stay. The usefulness of this proposal depends on how the web services is to function and if it is accepted (e.g. in relation to security requirements) to use a separate network. If data on the number of days is pushed out from the central system to a source available to external parties, border guards could possibly also access this information. Otherwise the OK/NOK response can be used to authorise the entry. The desk research on the web services should take this additional function into account.

8.4.3.4 Limited dataset – use as an exception

A proposal from the expert meeting was that a limited dataset (*i.e.* only alphanumeric data) might be used to register the individual file in the EES, in exceptional circumstances and if this measure would make for a more feasible solution in the electronic buffering. This solution would mean that the biometrics would have to be enrolled the next time the person crosses the border and added to the individual file.

8.4.4 Manual procedures

A business continuity plan, similar to the one outlined in this document, together with solutions for electronic and mobile buffering, mean that manual procedures should only be used in exceptional circumstances.

At the meeting held on 19 May 2015, some Member States' experts expressed the opinion that manual procedures, including stamping, should be included as a last resort when nothing else is possible.

If it is not possible to buffer and register data, the EES would have a missing entry/exit or, if the earlier crossing was the first crossing for the traveller, it would contain no data on the person.

In such a situation, three types of cases might have to be dealt with at the subsequent crossing:

1. *The traveller has a stamp indicating that the border was crossed even though the EES is missing the corresponding entry/exit record*

   The border guard could enter the missing entry or exit record separately, register the individual file where relevant, and also the entry/exit for the present border crossing made by the traveller. A notification system could serve as complementary information to ensure that the traveller's document was stamped at a BCP that had an outage of the EES.

2. *The traveller has no stamp and there is an entry or an exit missing in the EES*

   The border guard could do the same as above but would have to ask relevant questions to the traveller and rely on the information and supporting evidence (e.g. tickets) given by the traveller. In certain cases, there could be a specific reason why the traveller would be taken to a back office to answer those questions. In that case, a notification system would be even more helpful as complementary proof of the traveller's information. The Schengen Borders Code (Article 11) contains procedures and rules for how to handle a missing stamp. In general, these rules could be applicable to the case mentioned here.

3. *The EES indicates an overstayer*

   This can happen for both cases above. For case 2, it would be absolutely necessary to have a central recording of outages that matches the information given by the TCN as regards when and where an earlier crossing was made. The actions taken for case 1 and 2 could hopefully result in the EES data being complemented and the number of days for the total stay would then be recalculated automatically. If this is not possible, the person should be treated as an overstayer and any related complaints would have to be dealt with using manual procedures to be performed in a back office.

One Member State proposed a manual solution where the traveller receives a code that can be used at subsequent entry or exit. This would however rely on that power is available, where in most cases of this exceptional unavailability it is mentioned that the reason is interrupted power supply.

Besides the actions mentioned above, the border guard should make all the relevant registrations, identifications and verifications of the TCN, as is mentioned for the cases where electronic or manual buffering is possible, taking into account that an earlier border crossing is not recorded in the EES.

A status indication in the EES should accompany the retroactive entering of a missing entry/exit.

8.5 Business impact analysis

The business impact analysis below is a summary of the impact of different scenarios of EES unavailability for travellers and border guards. The analysis is built on the assumptions that solutions for electronic buffering would be implemented. For each scenario the impact is firstly described for the crossing when the EES was unavailable and secondly for the subsequent crossing.

Table 29 *Business Impact Analysis in case of EES unavailability*

	At entry	At exit
A: Electronic buffering and later registration of all data and biometrics is possible		
Impact on border guard (at crossing)	- No search can be made in the EES - No verification of number of days remaining for the authorised stay from the EES. The planned web interface could however be used to get this information if residing on a separate network. - Identification of TCNVEs (if first entry) is not possible - No registration of the individual file in the EES (if first entry) - No entry record is created	- No search can be made in the EES - No verification of number of remaining days from the EES. The planned web interface could however be used to get this information if residing on a separate network. - No exit record is created
Impact on traveller (at crossing)	- No information from the EES concerning the number of days remaining for authorised stay. The web interface could be used for delivering this information to the traveller.	- No information from the EES concerning the number of days remaining for authorised stay. The web interface could be used for delivering this information to the traveller.
Impact on border guard (at subsequent crossing)	- None. All data registered when the EES became available and the EES can be fully used.	- None. All data and biometrics registered when the EES became available and the EES can be fully used. - Possibly, for TCNVEs having made their first entry at the earlier crossing, the border guard would run an identification
Impact on traveller (at subsequent crossing)	- The lack of information as regards the number of days at the earlier crossing could result in the traveller mistakenly exceeding the number of days allowed. The web interface could be used for delivering this information to the traveller.	- The lack of information as regards the number of days at the earlier crossing could sometimes result in the traveller mistakenly exceeding the number of days allowed, *i.e.* he/she could forget the day of earlier crossing. The web interface could be used for delivering this information to the traveller.
B: No buffering and registration		
On border guard (at crossing)	Same as for Scenario A but for the possible addition of a stamp in the passport	Same as for Scenario 1 but for the possible addition of a stamp in the passport

On traveller (at crossing)	Same as for Scenario 1	Same as for Scenario 1
Impact on border guard (at subsequent crossing)	- An exit record would be missing in the EES. The border guard would have to add an exit record based on the stamp or on oral and other information from the traveller	- If the earlier crossing were a first entry there would be no data in the EES but possibly a stamp in the passport. - All additional checks and registrations normally done at entry would have to be done at exit. The border guard would have to add an entry record based on the stamp or on oral and other information from the traveller. - If the earlier crossing was not the first crossing, an entry record will be missing. The border guard would have to add an entry record based on the stamp or on oral and other information from the traveller.
Impact on traveller (at subsequent crossing)	- The lack of information as regards the number of days at the earlier crossing could result in the traveller mistakenly exceeding the number of days allowed. The web interface could be used for delivering this information to the traveller. - The duration of the border crossing could be longer than normal due to the need for the border guard to complete the EES data	- The lack of information as regards the number of days at the earlier crossing could result in the traveller mistakenly exceeding the number of days allowed. The web interface could be used for delivering this information to the traveller. - The duration could be longer than normal due to the need for the border guard to complete the EES data

9. VIS border check using travel document number

9.1 Introduction

This document presents a desk research aimed at assessing the feasibility of retrieving the visa information from VIS using the Travel Document Number (TDN) for verification at external border crossing point - instead of using the Visa Sticker Number (VSN), as it is currently the case.

Among other things it should be investigated whether this change will provide:

- The same information to border guards as when using the visa sticker number (VSN);
- The same information to the border guard when the visa stickers of members of a family are affixed on one travel document;
- A simplification of the border control process and a measurable decrease of duration when all other conditions remain equal.

It shall be noted that the current VIS legal basis[110] only allows the access to its data for verification at external border crossing points using the visa sticker number (in combination with the fingerprints for verification). Since the Pilot must not deviate from existing VIS legal basis the access to VIS using the Travel Document Number (TDN) cannot be tested in this Pilot. Therefore, the above points will be assessed from a desk research viewpoint.

9.1.1 Background and Objective

VIS central system offers a set of services (operations) that can be used by the Member States (via their national systems) to accomplish their business activities. Depending on the specific national authority accessing VIS and the business objective, a set of these operations can be used.

Currently, the following operations are available at VIS central level as far as border checks are concerned:

- **First line control operations in VIS**: an unique visa application is returned to the national system;
    - *AuthenticateByFingerprint*, *VerificationBorder* variant: the VSN together with 1-2-4 fingers are sent to VIS. In return, VIS delivers the information of the visa application record which has that VSN associated and whether the verification of the fingerprints has been successful or not (hit/no hit). This operation is processed by BMS system;
    - *Retrieval*, *VerificationBorder* variant: VIS receives a VSN and returns the unique visa application record which has that VSN associated.
- **Second line controls operations in VIS:**
    - *Search*, *IdentificationBorder* variant: alphanumeric search in VIS database, performed by the search engine. This operation allows data access with specified search fields but without a unique identifier. Each search variant either results in a no hit message, a hit list or a detailed record if only one match has been found.

[110] Art 18 of Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

Different types of searches can take place:

- Exact: the submitted search value exactly matches the value stored in VIS;
- Inexact: In cases where end-users do not know the exact value of a field, they can use the inexact search feature of the system to get a list of possible search candidates.

- *SearchByFingerprint*, *IdentificationBorder* variant: 1-10 fingers are sent to VIS, which are looked for in the whole biometric central database, involving BMS system. The VIS returns either a no hit message, a list of all visa applications that were found to match, or a detailed record if only one match has been found;
- *Retrieval*, *IdentificationBorder* variant: VIS receives a VSN or an application number and returns the visa application which has that VSN/application number associated.

Currently, both from a technical and a legal viewpoint, VIS consultation at first line control can only be performed using the VSN. This implies an extra step within the exiting border check process for the case of visa holders, as the visa sticker needs to be scanned for the VSN to be extracted automatically from the MRZ.

The following picture shows a general overview of the border check process for TCN, highlighting the extra step referred above:

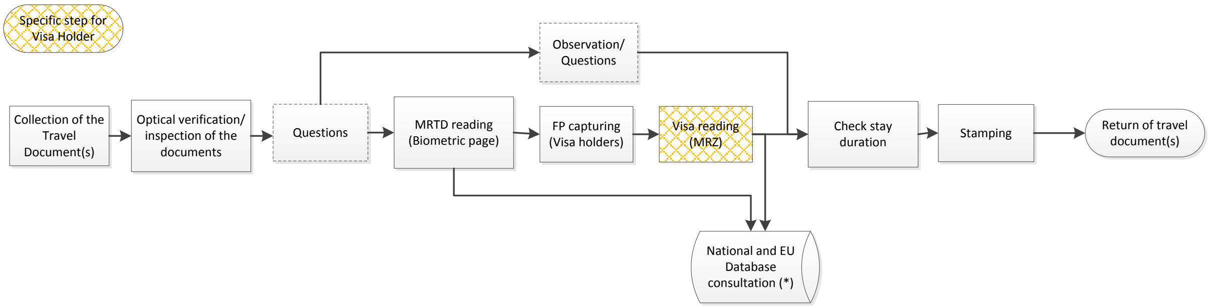

Specific step for Visa Holder
Observation/ Questions
Collection of the Travel Document(s)
Optical verification/ inspection of the documents
Questions
MRTD reading (Biometric page)
FP capturing (Visa holders)
Visa reading (MRZ)
Check stay duration
Stamping
Return of travel document(s)
National and EU Database consultation (*)

Figure 124 *Border check process steps*

9.2 Benefits and Challenges

From a business perspective, the following benefits can be derived by performing the VIS consultation by TDN:

- **Simplification of the border check process:** In case that the TDN could be used for the VIS consultation there would be no need to scan the Visa Sticker saving one step within the border clearance process for visa holders;
- **Reduce the end to end time:** by removing one of the steps of the current workflow, the total process would require less time. The time saved will vary depending on the specific national process, but it would be at least the scanning time, as the visa sticker will at any rate be manually checked;
- **Facilitate the automation:** the use of ABC gates or kiosks by the VH TCN would be simplified, as only the passport will have to be scanned. This would avoid confusions and difficulties in dealing with visa stickers;
- **Remove difficulties when scanning the visa sticker**, which are usually more frequent than for the passport scanning due to the different causes: visa sticker not properly placed in the passport page, problems with the ink, presence of stamps on top of the MRZ, etc;

- **Ease the implementation of systematic visa checks at exit**, which are voluntary at this point of time;
- **Enhanced security:** in those cases where the visa sticker cannot be properly scanned or when visas have been manually filled in.

On the other hand, the following challenges have been identified:

- **The TDN is not a unique identifier of the visa application**, as the relationship is not always one-to-one. Possible occurrences are:
    - Visa stickers of members of a family are simultaneously valid and affixed on one travel document;
    - Several Limited Territorial Validity (LTVs) are simultaneously valid and affixed on one travel document;
    - Several visa applications have been registered with the same travel document, even though only one visa is valid at a given time;
    - The Visa Sticker has been affixed to another TDN of the same person (*i.e.* a new passport has been issued as all pages of the previous one were full, previous travel document has expired, etc).
- **Data quality in VIS:** the travel document number has not been properly filled in and inserted in VIS when the visa was issued;
- Business logic is required so that the national system identifies from the MRZ in the travel document, whether a consultation to the VIS is required. This could be implemented both at central or national level, and in some cases the border guard decision should still take place as there are many exceptions. Systematic searches to VIS for all TCN shall not be allowed, as it will among other things overload VIS.

In light of the above constraints, it might be interesting to retain the possibility to still be able to consult VIS at the first line border check by using the VSN if desired as a fall back, as the relation between visa issued and visa sticker number is always one-to-one.

9.2.1 Technical options

As explained above, the current implementation of VIS does not have any operation which would always allow the retrieval of a visa record using the TDN.

The following technical alternatives have been identified:

9.2.1.1 Option 1: new Search operation combined with Database consultation

Description:

A search operation could be performed at first line using the existing search engine providing as search fields the TDN and the issuing authority.

1. In case there is only one hit for that search, that unique application record will be returned by the central system, and the information will be the same as it is currently the case using VSN.
2. In case there is more than one visa application registered in VIS for that TDN, a list containing all matching applications will be provided. Two options have been identified:
    a. Manually explored by the border guard to select the relevant application. Once an application is selected, then a retrieval operation is executed to recover all data of that specific visa application – by automatically using the VSN and thus the already existing *Retrieval-VerificationBorder* operation

b. Automatically processed, so that only the application records associated to a valid visa at the time the consultation is made are returned[111]. This information is available in the database.

   i. If there is only one record, *i.e.* only one application linked to a valid visa for a given TCN, all information of the same shall be returned to the border guard.

   ii. If there is more than one record for which the visa is valid (exceptional cases), then a list containing all of them should be returned.

   These cases will be considered as exceptions and will have to be further analysed by the border guard, in order to identify and retrieve the relevant visa record. Another possibility would be to rely on the fingerprints to identify the relevant record, as explained in Appendix 6 (10.6).

The following picture provides an overview of this option.

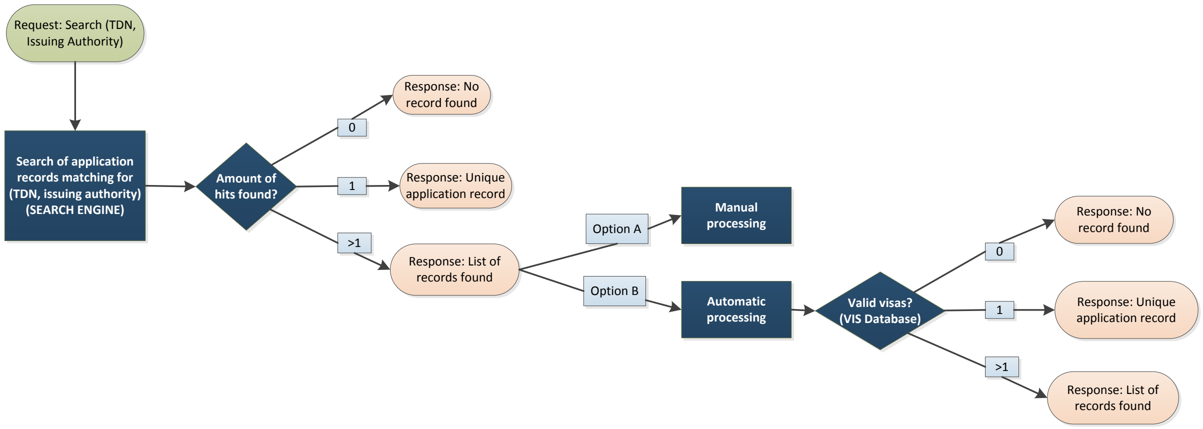

Request: Search (TDN, Issuing Authority)
Search of application records matching for (TDN, issuing authority) (SEARCH ENGINE)
Amount of hits found?
0
Response: No record found
1
Response: Unique application record
>1
Response: List of records found
Option A
Manual processing
Option B
Automatic processing
Valid visas? (VIS Database)
0
Response: No record found
1
Response: Unique application record
>1
Response: List of records found

Figure 125 *Technical option 1 description*

Advantages:

- For the first step above, an operation with the search functionality is already implemented at central level. Its execution needs to be however allowed at first line – for example by creating a *VerificationBorder* variant – and impose the use of TDN and issuing authority as search fields;
- The difference in the time it takes at central level to execute a retrieval compared to an exact search is negligible. Therefore, this first step above is expected to be as quick as the current consultation;
- The second step described above, if implemented automatically, would imply the modification of the VIS application, by triggering some processing and database queries. This modification is not complex, as the database does not need to be modified. The new search operation mentioned above has to include a second step to check in the VIS database which of the found applications have currently a valid visa. This information is already stored at Application level;
- In the cases where a unique record is returned, the information returned is exactly the same as for the currently existing VIS consultation by VSN;
- From a national system perspective, the impact of implementing this functionality is very low.

[111] The relevant table in the database has a foreign key that is the application id, and the query is not really impacting as it is indexed

Disadvantages:

- Some modifications are still needed at central and national side, as a new operation, even if very similar to existing ones, needs to be created;
- In case the second step is automated, this functionality shall be implemented as well at central level;
- The ICD and relevant documentation shall be updated accordingly;
- There will still be cases where the border guards will have to perform further steps/investigation. Those cases will be considered as exceptions;
- This approach will have an impact on the search engine as it will receive more requests. The current solution is supposed to be easily scalable, but the impact should be properly assessed;
- The current agreed SLA is higher for searches than for retrievals and should therefore be adapted to provide for the same short response time;
- The current allocation of the capacity in terms of operations per channel shall be revisited.

9.2.1.2 Option 2: Enhancement of the Search engine

Description:

A (new) search operation could be performed against the existing search engine using as search fields the TDN together with the issuing authority, while filtering only those applications that have an issued visa which is valid at the time of the consultation. The result could be either no application record, all the information of an application if one unique hit is found, or a list of hits.

This configuration will limit or even reduce those cases when more than one application is found and a list is thus returned. Therefore, as there would be only one hit in the vast majority of cases, the central system would in these cases return the application record information.

To achieve this goal however, the current visa engine needs to be modified to include more fields – such as for example, the expiration date of the visa[112] or other fields related to the Decision made on the visa application – and the VIS application needs to be modified accordingly to be able to feed this new information in the search engine.

The following picture provides an overview of this option

[112] The expiration date is always present in the visa application, as it is automatically calculated based on the start of validity date.

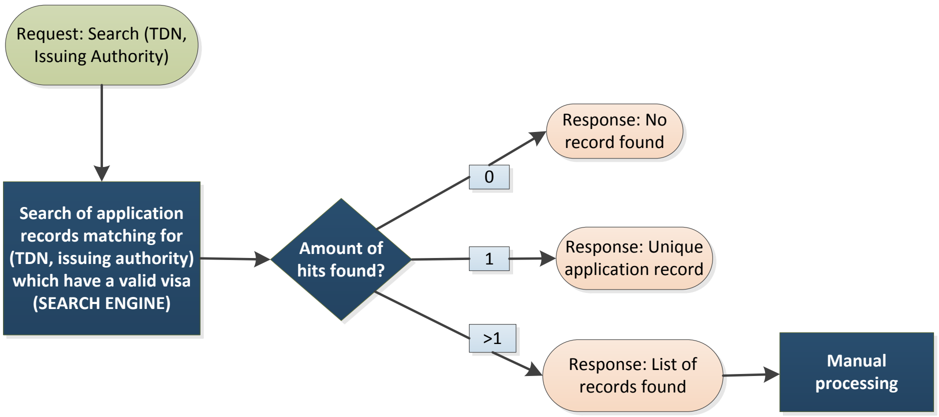

Request: Search (TDN, Issuing Authority)
Search of application records matching for (TDN, issuing authority) which have a valid visa (SEARCH ENGINE)
Amount of hits found?
0
1
>1
Response: No record found
Response: Unique application record
Response: List of records found
Manual processing

***Figure 126** Technical option 1 description*

Advantages:

- The central system will almost always return one unique application in one step, containing the same information as the current consultation by VSN;
- The difference in the time it takes at central level to execute a retrieval compared to an exact search is negligible;
- The impact at the national system is low;
- The search engine is more efficient and performant than querying the database, especially for exact searches.

Disadvantages:

- The search engine needs to be reconfigured to include more fields, which will have an impact that needs to be properly assessed;
- The application needs to be changed and adapted to be able to feed the search engine with this new information that has to be stored systematically when visas are issued. The impact of this change should be assessed, but is expected to be major, as many tables will have to be queried and the search engine will have to be updated for each visa decision;
- Those exceptional cases where several visas are simultaneously valid and affixed to one travel document shall be at any rate treated as exceptions;
- The current allocation of the capacity in terms of operations per channel shall be revisited.

9.2.1.3 Option 3: Re-design of the VIS Database

Description

A new Data Model could be designed and implemented to enable querying the database by TDN – probably combined with the IssuingAuthority or other fields.

Advantages

- A new retrieval operation similar to the existing one could be implemented afterwards.

Disadvantages

- Major change in the current VIS implementation;

- Potential side effects in the rest of VIS functionality.

9.3 Preliminary observations

The table below compares the three options explained above, scoring the advantages from 1 (lower) to 5 (higher).

Table 30 *Comparison between the options*

Option	Complexity of Implementation	Performance	Impact on current VIS
Option 1: new Search operation combined with Database consultation	4 (modification of VIS application to trigger a query to the database in specific cases)	3 (both search engine and database are involved)	4
Option 2: Reconfiguration Enhancement of the Search engine	3 (modification of the search engine to include more fields and modification of VIS application to feed the Search engine)	5 (only the search engine is involved in the execution)	4
Option 3: Re-design of the VIS Database	4 (complete change of VIS Data model)	3	1

Out of the above explained options, the alphanumeric search engine solution in VIS is proven to be very efficient and performant and should therefore be the preferred option from a technical perspective, above the option of increasing the amount of queries to the database. Therefore, technical option 2 would be the preferred one:

- For those cases where one TDN issued by a given authority only has one valid visa associated, the same information will be returned to the border guard as when the consultation is done with the VSN;
- Those cases where there are several valid visas affixed to the same TDN, or where the traveller has a new TDN while the visa is affixed to a previous one, will need to be treated as exceptions and be further analysed by the border guards;
- Impact on the current system shall be further assessed:
    - Major adaptation and modification both at VIS and national system level are required, even if these are not estimated to be very impacting as most of the functionality is already implemented. This will as well imply a modification of the ICD;
    - The current capacity allocation per VIS channels shall be revisited;
    - Search engine capacity shall be revisited;
    - Increase of time if any due to the fact that an exact search instead of a retrieval will be performed. The current contractual SLAs are different for each type of operation.

10. Appendices

10.1Appendix 1: Abbreviations

ABC	Automated Border Control. Also referred to as e-Gates or electronic gates
AFIS	Automated Fingerprint Identification System
BAC	Basic Access Control
BCP	Border Crossing Point
BG	Border Guard
BMS	Biometric Matching System
CMC	Cumulative Matching Characteristic Curve
COM	European Commission
COTW	Clock On The Wall
CRL	Control Revocation List
CSCA	Country Signing Certificate Authority
DET	Detection Error Trade-off
DG2	DataGroup 2
EAC	Extended Access Control
EES	Entry-Exit System
e-MRTD	Electronic MRTD (see below MRTD)
EP	European Parliament
FAR	False Acceptance Rate
FI	Facial Image(s)
FMR	False Match Rate
FNIR	False Negative Identification Rate
FNMR	False non-Match Rate
FP	Fingerprint(s)
FPIR	False Positive Identification Rate
FRR	False Rejection Rate
FTA	Failure to Acquire
ICAO	International Civil Aviation Organisation
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone of a Machine Readable Travel Document
MS	EU Member State(s)
NDPA	National Data Protection Authority
NFIQ	NIST Fingerprint Image Quality
NIST	National Institute of Standards and Technology

NUI	National Uniform Interface
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PKD	Public Key Directory
PM	Project Manager
PoC	Proof of Concept
QA	Quality Assurance
QC	Quality Control
ROC	Receiver Operating Characteristic
RT	Registered Traveller
RTP	Registered Traveller Programme
SAC	Supplemental Access Control
SLA	Service Level Agreement
SOD	Document Security Object
SIS II	Schengen Information System of the 2nd Generation
TC	Test Case
TCN	Third Country National
TCNVE	Third Country National – Visa Exempt
TCNVH	Third Country National – Visa Holder
TDN	Travel Document Number
ToR	Terms of Reference
UPS	Uninterruptible Power Supply
VE	Visa Exempt
VH	Visa Holder
VIS	Visa Information System
VSN	Visa Sticker Number

10.2Appendix 2: Glossary

10.2.1 ISO standard glossary

In general, we use the biometric vocabulary as defined in ISO standards such as ISO/IEC 2382-37:2012 'Information technology – Vocabulary – Part 37: Biometrics', and ISO/IEC 19795 'Information technology — Biometric performance testing and reporting — Part 1: Principles and framework'. In case a specific term is not included in ISO/IEC 2382, we use ISO/IEC 19795-1.

For convenience of the reader, we introduce the key terms and their source below.

Acquisition

Failure To Acquire (FTA): proportion of a specified set of biometric acquisition processes that were failures to acquire (ISO/IEC 2382).

Failure To Enrol (FTE): proportion of a specified set of biometric enrolment transactions that resulted in a failure to enrol (ISO/IEC 2382).

Matching in general – attempt based

Matching performance – attempt-based, is expressed as:

False Match Rate (FMR): proportion of the completed biometric non-mated comparison trials that result in a false match (ISO/IEC 2382).

False non-Match Rate (FNMR): proportion of the completed biometric mated comparison trials that result in a false non-match (ISO/IEC 2382).

Matching for verification:

False Acceptance Rate (FAR): proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed (ISO/IEC 19795-1). The term ferrfake can also be used.

False Rejection Rate (FRR): proportion of verification transactions with truthful claims of identity that are incorrectly denied (ISO/IEC 19795-1). The term ferrlive can also be used.

10.2.2 General glossary

Basic Access Control: challenge-response protocol where a machine reader must create symmetric key in order to read the contactless chip by hashing the data scanned from the MRZ.

Check Duration: time to perform Passive Authentication (including background system query).

Check Process time: complete checking process (starting from optical reading trigger to end of check).

Clock On The Wall: a timekeeper (border guard or assisting personnel) manually measuring the time, using a stopwatch or specific software.

End to end duration: the duration of the entire border crossing process, from the moment the traveller cross the yellow line until the border crossing.

Extended Access Control: protection mechanism for additional biometrics included in the e-MRTD. The mechanism will include State's internal specifications or the bilateral agreed specifications between States sharing this information.

Full Frontal: this type of Face Image Type includes the full head with all hair in most cases, as well as neck and shoulders

Minutiae: specific points in a finger image.

Passive Authentication: verification mechanism used to check if the data on the RF chip of an e-MRTD is authentic and unforged by tracing it back to the Country Signer Certificate Authority (CSCA) certificate of the issuing country.

Reading Duration: time to read all files from chip (EF.COM, EF.SOD, DG1, DG2, conditionally DG14, DG15).

Token Frontal: a Face Image Type that specifies frontal images with a specific geometric size and eye positioning based on the width and height of the image.

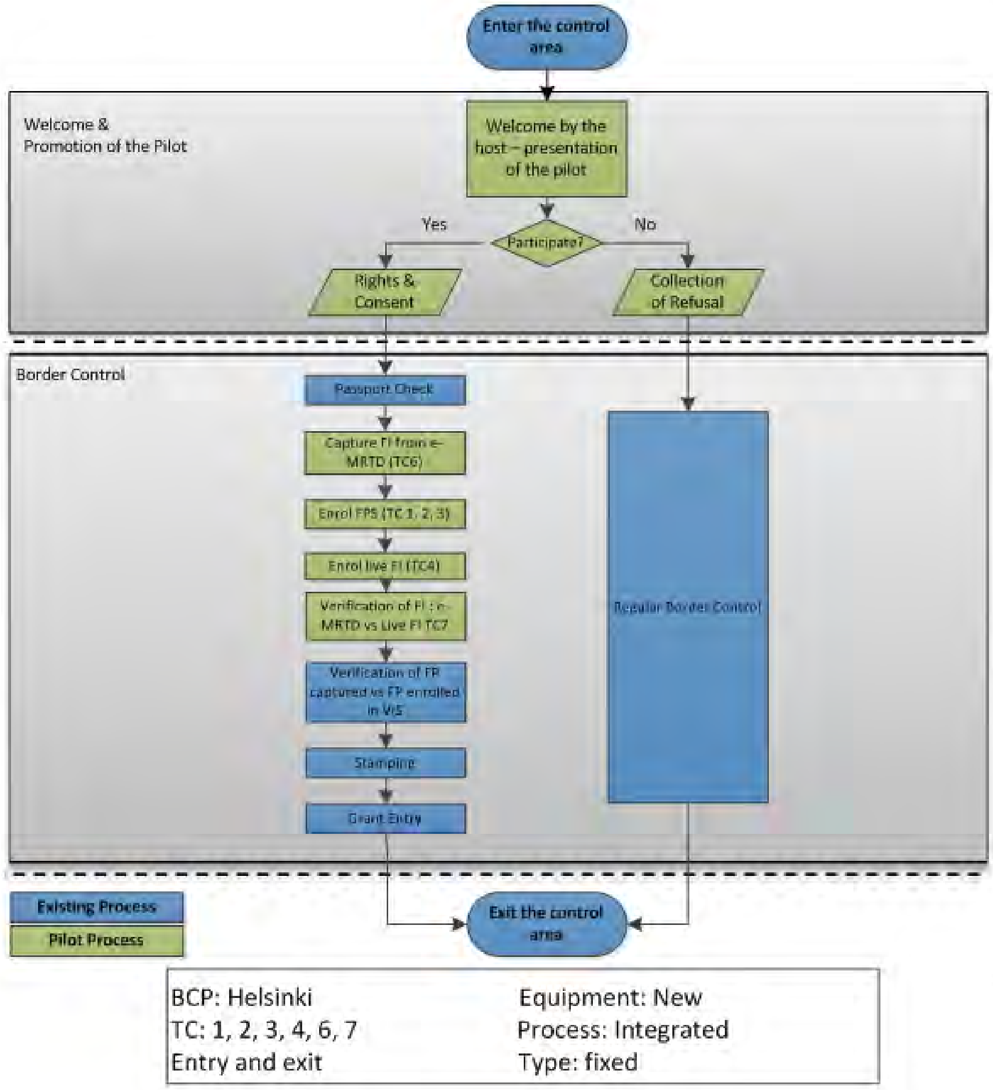
10.3 Appendix 3: Fingerprints

10.3.1 Descriptions of the testing processes

Helsinki

The Pilot was executed in the West Terminal of Helsinki Port, in Finland. There were two dedicated lanes used for TCs executed in the manual booth, one of which was set up at entry and another at exit.

As presented in the figure below, the Pilot process was integrated in the existing border check process. Test cases of FP enrolment (TC1, TC2, TC3) were executed sequentially, whereas test cases of live FI enrolment (TC4), FI capture from e-MRTD (TC6) and FI verification (TC7) were executed in parallel with FP enrolment.



BCP: Helsinki
TC: 1, 2, 3, 4, 6, 7
Entry and exit

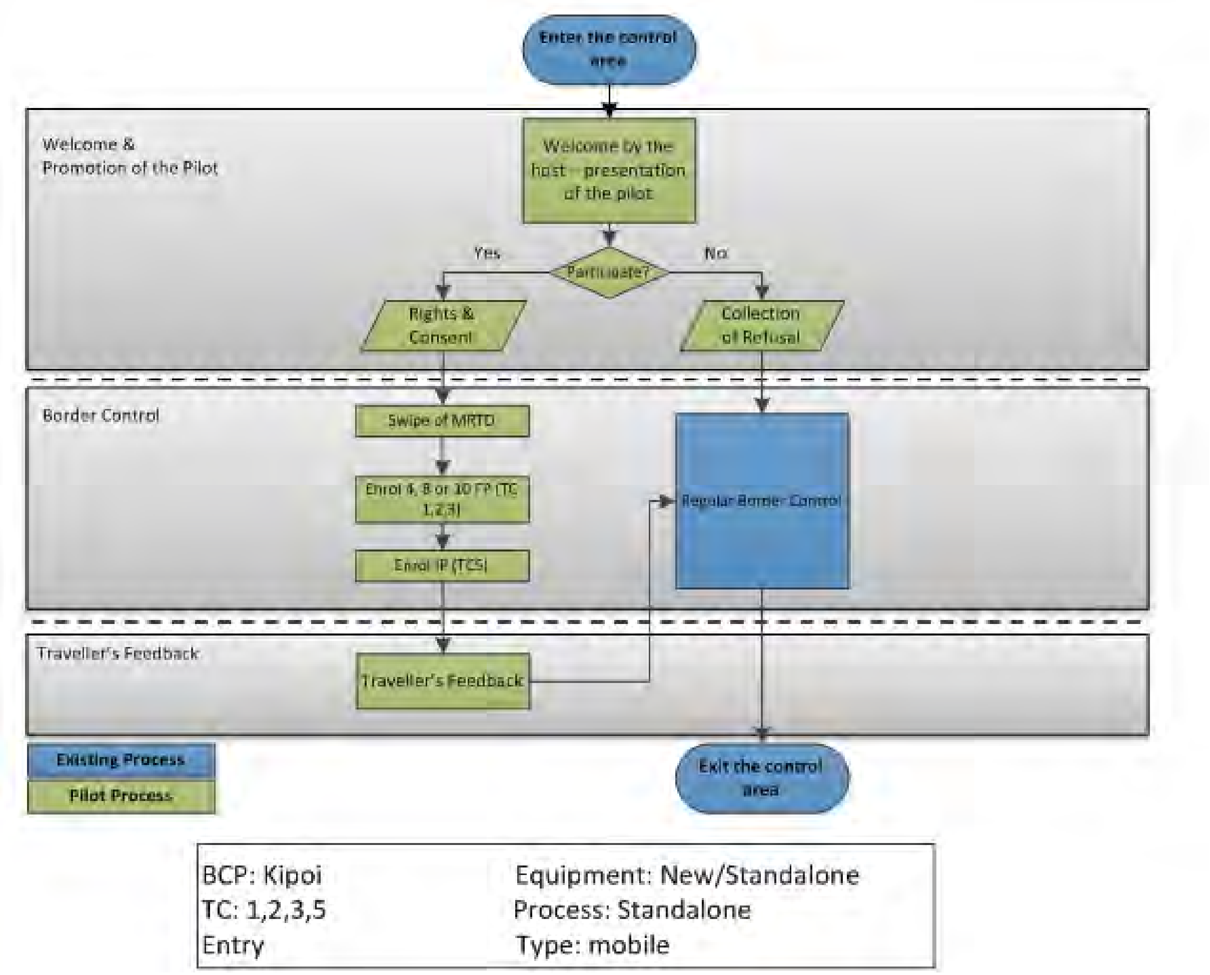
Equipment: New
Process: Integrated
Type: fixed

Figure 127 *Steps of the existing and the Pilot processes in Helsinki for TCs executed in the manual booth*

Kipoi

The Pilot was carried out at the entry of the land border BCP in Kipoi, Greece. There was no dedicated lane for the testing, but rather the whole area around the BCP was used, as the testing was executed with mobile, stand-alone equipment.

The comparison of the Pilot testing process with the existing border check process is shown in the figure below, indicating detailed process steps. The test cases of FP enrolment (TC1, 2, 3) were executed sequentially, whereas the test case of iris enrolment (TC 5) was executed in parallel with FP enrolment.



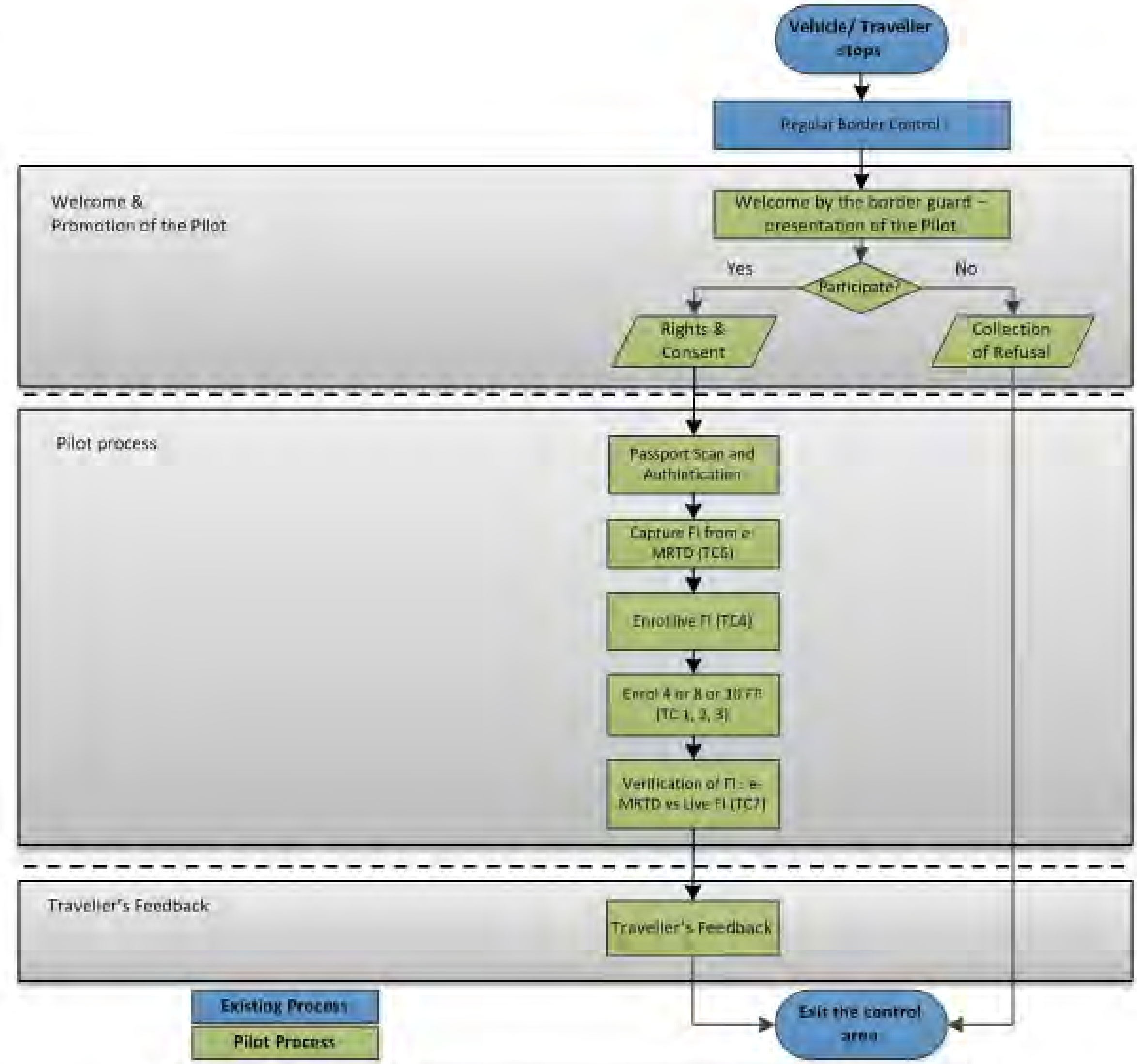
BCP: Kipoi	Equipment: New/Standalone
TC: 1,2,3,5	Process: Standalone
Entry	Type: mobile

***Figure 128** Steps of the existing and the Pilot processes in Kipoi*

Vaalimaa

The Pilot was executed at the entry and exit of the land border BCP in Vaalimaa, Finland. There were two dedicated lanes used for the Pilot, one of which was set up at entry and another at exit.

The Pilot process was introduced after the existing border check process. Test cases of FP enrolment (TC1, TC2, TC3) were executed sequentially, whereas test cases of live FI enrolment (TC4), FI capture from e-MRTD (TC6) and FI verification (TC7) were executed in parallel with FP enrolment. The comparison of the Pilot testing process with the existing border check process is shown in the figure below, indicating detailed process steps of all TCs.


Vehicle/ Traveller stops
Regular Border Control
Welcome & Promotion of the Pilot
Welcome by the border guard – presentation of the Pilot
Yes
No
Participate?
Rights & Consent
Collection of Refusal
Pilot process
Passport Scan and Authinfication
Capture FI from e-MRTD (TC6)
Enrol live FI (TC4)
Enrol 4 or 8 or 10 FP (TC 1, 2, 3)
Verification of FI : e-MRTD vs Live FI (TC7)
Traveller's Feedback
Traveller's Feedback
Existing Process
Pilot Process
Exit the control area

BCP: Vaalimaa	Equipment: New / Integrated
TC: 1, 2, 3, 4, 6, 7	Process: after regular border check
Entry, exit	Type: fixed

Figure 129 Steps of the existing and the Pilot processes in Vaalimaa

10.4 Appendix 4: Facial Image

10.4.1 E-MRTD chip data structure

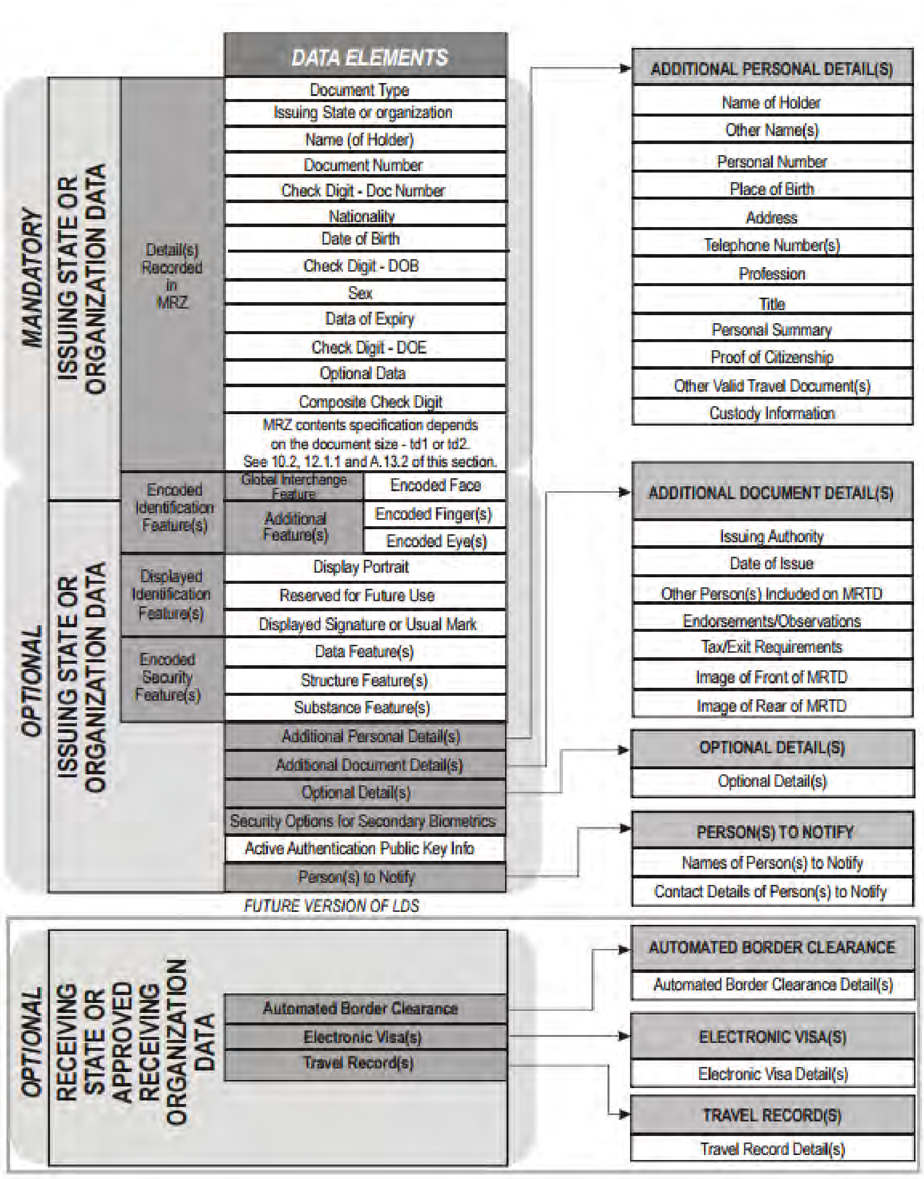

DATA ELEMENTS
MANDATORY
ISSUING STATE OR ORGANIZATION DATA
Detail(s) Recorded in MRZ
Document Type
Issuing State or organization
Name (of Holder)
Document Number
Check Digit - Doc Number
Nationality
Date of Birth
Check Digit - DOB
Sex
Data of Expiry
Check Digit - DOE
Optional Data
Composite Check Digit
MRZ contents specification depends on the document size - td1 or td2. See 10.2, 12.1.1 and A.13.2 of this section.
OPTIONAL
ISSUING STATE OR ORGANIZATION DATA
Encoded Identification Feature(s)
Global Interchange Feature
Encoded Face
Additional Feature(s)
Encoded Finger(s)
Encoded Eye(s)
Displayed Identification Feature(s)
Display Portrait
Reserved for Future Use
Displayed Signature or Usual Mark
Encoded Security Feature(s)
Data Feature(s)
Structure Feature(s)
Substance Feature(s)
Additional Personal Detail(s)
Additional Document Detail(s)
Optional Detail(s)
Security Options for Secondary Biometrics
Active Authentication Public Key Info
Person(s) to Notify
FUTURE VERSION OF LDS
OPTIONAL
RECEIVING STATE OR APPROVED RECEIVING ORGANIZATION DATA
Automated Border Clearance
Electronic Visa(s)
Travel Record(s)
ADDITIONAL PERSONAL DETAIL(S)
Name of Holder
Other Name(s)
Personal Number
Place of Birth
Address
Telephone Number(s)
Profession
Title
Personal Summary
Proof of Citizenship
Other Valid Travel Document(s)
Custody Information
ADDITIONAL DOCUMENT DETAIL(S)
Issuing Authority
Date of Issue
Other Person(s) Included on MRTD
Endorsements/Observations
Tax/Exit Requirements
Image of Front of MRTD
Image of Rear of MRTD
OPTIONAL DETAIL(S)
Optional Detail(s)
PERSON(S) TO NOTIFY
Names of Person(s) to Notify
Contact Details of Person(s) to Notify
AUTOMATED BORDER CLEARANCE
Automated Border Clearance Detail(s)
ELECTRONIC VISA(S)
Electronic Visa Detail(s)
TRAVEL RECORD(S)
Travel Record Detail(s)

Figure 130 *Mandatory and optional Data Elements defined for LDS*

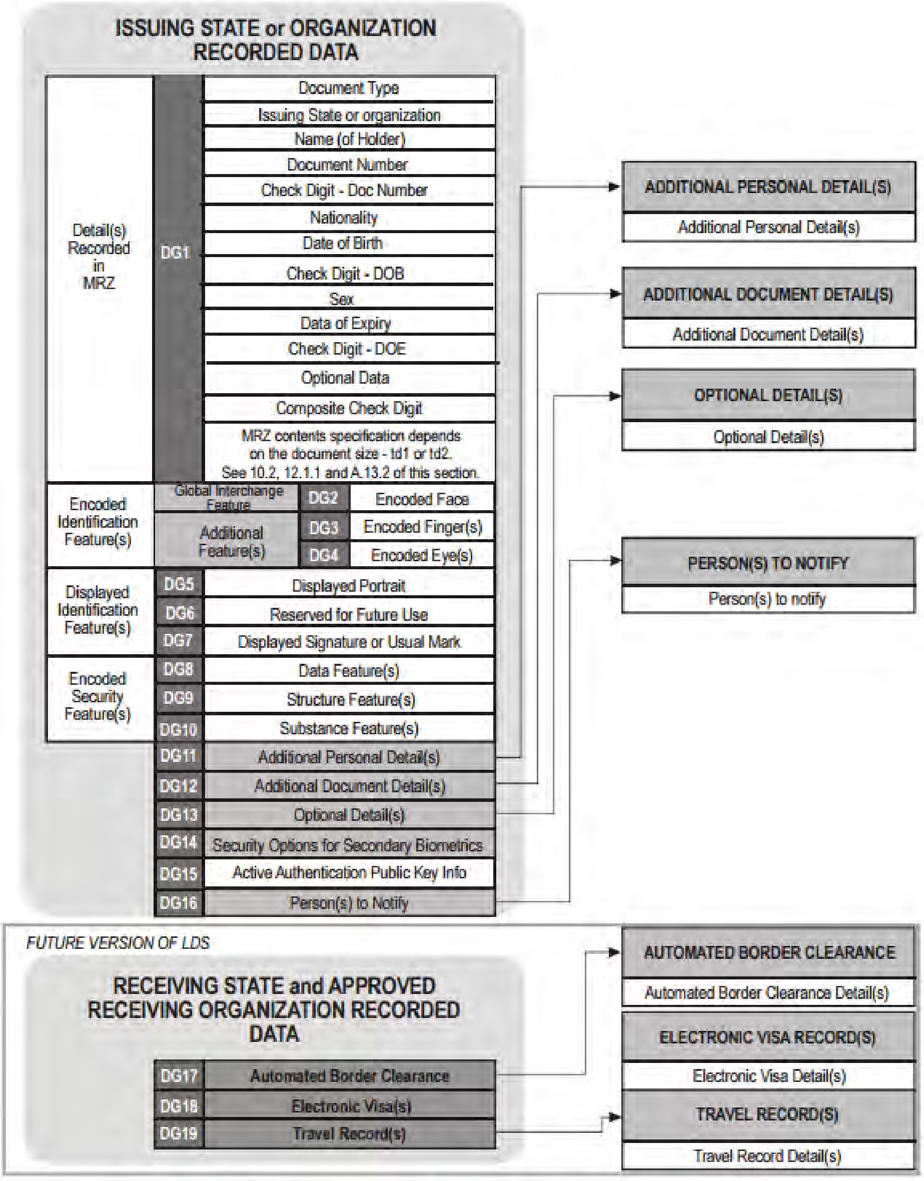

ISSUING STATE or ORGANIZATION RECORDED DATA
Detail(s) Recorded in MRZ
DG1
Document Type
Issuing State or organization
Name (of Holder)
Document Number
Check Digit - Doc Number
Nationality
Date of Birth
Check Digit - DOB
Sex
Data of Expiry
Check Digit - DOE
Optional Data
Composite Check Digit
MRZ contents specification depends on the document size - td1 or td2. See 10.2, 12.1.1 and A.13.2 of this section.
Encoded Identification Feature(s)
Global Interchange Feature
Additional Feature(s)
DG2
Encoded Face
DG3
Encoded Finger(s)
DG4
Encoded Eye(s)
Displayed Identification Feature(s)
DG5
Displayed Portrait
DG6
Reserved for Future Use
DG7
Displayed Signature or Usual Mark
Encoded Security Feature(s)
DG8
Data Feature(s)
DG9
Structure Feature(s)
DG10
Substance Feature(s)
DG11
Additional Personal Detail(s)
DG12
Additional Document Detail(s)
DG13
Optional Detail(s)
DG14
Security Options for Secondary Biometrics
DG15
Active Authentication Public Key Info
DG16
Person(s) to Notify
ADDITIONAL PERSONAL DETAIL(S)
Additional Personal Detail(s)
ADDITIONAL DOCUMENT DETAIL(S)
Additional Document Detail(s)
OPTIONAL DETAIL(S)
Optional Detail(s)
PERSON(S) TO NOTIFY
Person(s) to notify
FUTURE VERSION OF LDS
RECEIVING STATE and APPROVED RECEIVING ORGANIZATION RECORDED DATA
DG17
Automated Border Clearance
DG18
Electronic Visa(s)
DG19
Travel Record(s)
AUTOMATED BORDER CLEARANCE
Automated Border Clearance Detail(s)
ELECTRONIC VISA RECORD(S)
Electronic Visa Detail(s)
TRAVEL RECORD(S)
Travel Record Detail(s)

Figure III-2. Data group reference numbers assigned to LDS

Figure 131 *Data group reference numbers assigned to LDS*

Source: ICAO, Machine Readable Travel Documents, Part 3 Machine Readable Official Travel Documents

10.4.2 Chip reading procedure

The steps in reading a FI from a chip embedded in an eMRTD as per ISO/IEC 14443 and ISO/IEC 7816-4 are described below. The most right column describes possible reasons for failing to read the FI from the chip.

Table 31 *Steps in reading a FI from a chip embedded in an e-MRTD*

Step#	What	Possible reasons for failing to read the FI from the chip
Part 1	**Initialisation between chip and reader.** Summary as per ISO/IEC 14443-3 Type A. Type B is functionally equivalent but uses a different modulation.	
1.1	eMRTD with embedded and personalised chip is moved into the field emitted by the ISO/IEC 14443 compatible reader (part of the Inspection System)	
1.2	Once the chip has harvested enough energy, its operating state is IDLE, in which it will only respond to REQA (request type A) or WUPA (wake-up type A, to wake-up from a previous HALT command) commands from the reader.	If chip and/or reader do not comply with the required ISO standards, the initialisation will fail. Subsequently reading the FI from the chip will not be possible. The same holds in case the chip, the antenna or the link between chip and antenna are defect.
1.3	Upon recognition of such a REQA or WUPA command, the operating state of the chip will change into READY and the chip will send an ATQA response to the reader.	
1.4	Upon reception of the ATQA response from the chip, the reader starts the anti-collision management sequence and sends a SELECT command to the reader to obtain the UID (Unique Identifier) from the chip	
1.5	Upon reception from the UID, the reader issues a SELECT command including the UID, to which the chip answers with a SAK (Select Acknowledge) response.	
1.6	[In case of collision detection, the reader will issue ANTICOLLISON commands to resolve the collision]	If multiple chips respond and the anti-collision fails, it will not be possible to initialise communication with the chip (and subsequently read the FI from the chip).
1.7	Once the chip received the appropriate SELECT command and any collisions are resolved, the chip changes its state to READY	
Part 2	**Activation of the communication between chip and reader conform to ISO/IEC 14443-4 and ISO/IEC 7816-4** In the READY state, communication between chip and reader is done conform to ISO/IEC 14443-4. Higher protocol level commands as per ISO/IEC 7816-4 will now be processed by the chip	
2.1	Activation of the link and negotiation of frame size, bitrate, waiting time etc. The terminal sends a Request for Answer to Select	

	(RATS) command	
2.2	The chip answers with an Answer to Select (ATS) response The negotiation yields a 4 layer communication model (physical, data link, session and application layer).	
2.3	Between chip and reader, Application Protocol Data Units (APDUs) conform to ISO7816-4 are now exchanged. The ICAO eMRTD issuing State Application is selected.	
2.4	The Elementary Files (EFs) of the required Data Groups (DGs) are read from the LDS. This is done using SELECT and READ BINARY commands. First EF.COM is read, whose tag list contains the DGs (stored in their EFs) that are available. Each EF is then read out to obtain the DG. The MRZ is normally the first EF read.	
2.5	**Passive Authentication (required)** EF.SOD is read to allow the verification of the integrity of the EFs read. The IS verifies this integrity. Specified in [ICAO9303P3V2] Section 7 Specifications, Subsection 7.2 Inspection. Elaborated in [FTXBPGABCT].	For the IS to verify this integrity the Document Signer's Public Key is required. This key should be obtained in a certificate from the PKD and stored in the IS. In case it is provided in the chip, the certificate may also be read from there. The IS should verify the certificate containing the DS Public Key using the Issuing State's Country Signing CA Public Key from a corresponding certificate.. The verification of the integrity of the EFs will fail if either or both of these certificates are not available, or are revoked.
2.6	Further processing is dependent upon the design of the IS application, and may involve: • BAC (optional) • AA (optional) • EAC (optional) • Decryption of additional biometrics (optional) This optional processing involves ISO/IEC 7816-4: • EXTERNAL AUTHENTICATE • INTERNAL AUTHENTICATE	

	• GET CHALLENGE	
Part 3	**BAC (Basic Access Control) – optional**	
3.1	IS reads MRZ optically and uses SHA-1 to derive the BAC keys. IS' MRZ reader might fail (in which case data entry might be done via keyboard if this is available, and supported by the IS application)	Both OCR and keyboard entry may fail. For those eMRTDs that implement BAC, the reading will then fail.
3.2	The IS and chip mutually authenticate and derive session keys.	
3.3	After successful authentication, secure messaging is available between IS and chip.	
Part 4	**AA (Active Authentication) – optional**	
	AA consists of a challenge-response between reader and chip using a chip-specific public key pair. AA must be preceded by PA. The PA ensures that the chip's public key for AA is authentic and unchanged. The challenge-response protocol will ensure the chip is genuine and matches the data page.	For eMRTDs that implement AA, failure of a successful AA execution may be taken into consideration by the IS when processing information from the eMRTD such as FI. This may lead to unavailability/rejection of the FI
Part 5	**EAC (Extended Access Control) – optional**	
	This depends on the issuing State's internal specification or on the bilateral specifications between cooperating States. This is not relevant for reading the FI.	
Part 6	**Decryption**	
	This depends on the issuing State's internal specification or on the bilateral specifications between cooperating States. This is not relevant for reading the FI.	

10.4.3 German statistics on reading and validating eMRTDs

Germany shared statistics with eu-LISA, based on operating their Inspection Systems. These statistics address multiple topics (usage of cryptographic protocol, verifiability of eMRTDs, and duration) across all TCN travellers and the period from 01.01.2015 to 31.05.2015. As these topics are closely related the information was grouped together and included in the section on the 'Added complexity of PA'.

10.4.4 References with regard to reading the FI from the chip

Smartcard and RFID

[Finkenzeller] RFID Handbuch, by Klaus Finkenzeller, including NFC (in German), ISBN 978-3-446-41200-2.

[RanklEffing] Handbuch der Chipkarten, by Wolfgang Rankl & Wolfgang Effing (in German), ISBN 3-446-22036-4.

[MayesKonstantinos] Smart Cards, Tokens, Security and Applications, by Keith Mayes & Konstantinos Markantonakis (editors, RHUL Smart Card Centre), (2008), ISBN 978-0-387-72197-2.

[Hendry] Smart Card Security and Applications, by Mike Hendry, 2001, ISBN 1-58053-156-3.

ICAO

[ICAO9303P1V2] ICAO Doc 9303 Part 1 Machine readable passports Volume 2 Specifications for electronically enabled passports with biometric identification capability (2006)

[ICAO9303P3V2] ICAO Doc 9303 Part 3 MRTD Volume 2 MRD with biometrics (2008)

[ICAO9303SUP] Supplement to Doc 9303 Version: Release 14 Status: Final (2014)

Frontex

[FTXBPGABCD] Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems (2011)

[FTXBPGABCT] Best Practice Technical Guidelines for Automated Border Crossing Systems (2012)

[FTXBPGABCO] Best Practice Operational Guidelines for Automated Border Crossing Systems (2012)

[FTXBIOP1] BIOPASS – Study on Automated Border Crossing systems for Registered Passengers at Four European Airports

[FTXBIOP2] BIOPASS II – Automated Biometric Border Crossing Systems Based on Electronic Passports and Facial Recognition: RAPID and SmartGate

[FTXNEES] National Entry Exit Systems Study (2013)

[FTXETHCS] Ethics of border control

[FTXACM] Anti-corruption measures in EU border control.

[FTXOTEP] Operational and Technical security of Electronic Passports, Warsaw, July 2011

10.4.5 References with regard to the complexity of Passive authentication

Cryptographic basis

- Cryptography - theory and practice, by D. Stinson, ISBN 0-8493-8521-0.
- Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot and S. Vanstone, ISBN 0-8493-8523-7.

Foundation reading material with regard to chip cards:

- RFID Handbuch, by Klaus Finkenzeller, including NFC (in German), ISBN 978-3-446-41200-2.
- Handbuch der Chipkarten, by Wolfgang Rankl & Wolfgang Effing (in German), ISBN 3-446-22036-4.
- Smart Cards, Tokens, Security and Applications, by Keith Mayes & Konstantinos Markantonakis (editors, RHUL Smart Card Centre), (2008), ISBN 978-0-387-72197-2.
- Smart Card Security and Applications, by Mike Hendry, 2001, ISBN 1-58053-156-3.

Other:

[PRESSURV] – Council of the European Union, Brussels, 2 April 2014, 7317/14, FAUXDOC 9

COMIX 138.

Plus the same publications that are referenced in the 'Facial image reading from the chip' section.

10.4.6 German statistics on reading and validating eMRTDs

At German border control locations that are operated by the German Federal Police, machine assisted document inspection systems are used to check authenticity, integrity and validity of MRTD documents. During this checking process the systems log diverse data. For each transaction one log is created. The logging format is defined in XML scheme according to the Technical Guideline BSI TR-03135. The used data as basis for the statistics throughout this document were accumulated in the period time from 01.01.2015 to 31.05.2015.

The information can be summarised as:

Logs with ePassport - completely read*	3.580.974
Logs with ePassport - completely read* – third countries** (TC)	1.437.003
Countries seen at German Borders:	200
-> Therefrom countries issuing ePassports:	112
-> Therefrom countries on the German Master List (ML):	63
-> Therefrom third countries (TC) on ML:	31
Third countries (TC) issuing ePassports seen at German Borders:	80
Successfully read and PA verified ePassports from Schengen Countries:	2.138.484
Successfully read and PA verified ePassports from third country nationalities (TCN):	1.232.408

Legend:

* at least SOD, DG1 and DG2 read

** TCN = not member from EU/EEA/CH

Usage of the different cryptographic protocols

This table below shows the distribution of the usage of different crypto protocols of all ePassport issuing third countries (TC). Except NGA each country uses BAC. **45** countries support CA, whereas **24** countries support AA. **7** countries support both depending on the different passport generations, **18** support neither CA nor AA.

Note that CMR is only included here, but not in the following sheets, because DG1, DG2 cannot be read from CMR passports.

Table 32 *Distribution of the usage of different crypto protocols of all ePassport issuing third countries*

Country Code 3-letter	CSCA available? (DE ML)	Crypto protocol			Comments
		BAC	CA	AA	
ALB	0	x	x	x	depending on passport generation
AND	0	x	x	/	
ARE	1	x	x	/	
ARG	1	x	/	x	
ARM	0	x	x	/	
AUS	1	x	/	x	
AZE	1	x	x	/	
BDI	0	x	x	/	
BEN	0	x	x	/	
BHS	0	x	/	x	
BIH	0	x	x	/	
BRA	0	x	x	/	
BRN	0	x	/	/	
BWA	0	x	x	/	
CAF	0	x	/	/	
CAN	1	x	/	x	
CHL	1	x	x	/	
CHN	1	x	x	x	depending on passport generation
CIV	0	x	/	x	
CMR	0	x	/	/	
COG	0	x	/	/	
COM	0	x	x	/	
DZA	0	x	x	/	
GAB	0	x	x	/	
GEO	0	x	x	/	
GIN	0	x	/	x	
GMB	0	x	x	/	
GNB	0	x	/	/	
IDN	0	x	x	/	
IND	0	x	/	/	
IRN	0	x	x	x	depending on passport generation
ISR	1	x	x	/	
JPN	1	x	/	x	
KAZ	1	x	/	x	
KHM	0	x	x	/	
KNA	0	x	/	x	
KOR	1	x	x	/	
LSO	0	x	/	/	
MAR	0	x	x	x	depending on passport generation

MCO	1	x	/	x	
MDA	1	x	x	/	
MDG	0	x	x	/	
MDV	0	x	/	x	
MKD	1	x	x	/	
MNE	0	x	x	/	
MNG	0	x	x	/	
MOZ	0	x	x	/	
MRT	0	x	x	/	
MYS	1	x	x	x	depending on passport generation
NER	0	x	x	/	
NGA	0	/	/	/	
NZL	1	x	/	x	
OMN	0	x	x	/	
PAN	0	x	/	x	
PHL	0	x	/	x	
QAT	1	x	/	/	
RKS	0	x	x	/	
RUS	1	x	x	/	
SDN	0	x	/	/	
SEN	0	x	x	x	depending on passport generation
SGP	1	x	/	/	
SMR	0	x	/	/	
SOM	0	x	x	x	depending on passport generation
SRB	1	x	x	/	
SSD	0	x	/	/	
TGO	1	x	/	x	
THA	1	x	/	/	
TJK	1	x	x	/	
TKM	0	x	/	/	
TUR	1	x	/	x	
TWN	1	x	/	/	
UKR	0	x	x	/	
UNO	1	x	/	/	
USA	1	x	/	/	
UZB	0	x	x	/	
VAT	1	x	x	/	
VCT	0	x	/	x	
VEN	1	x	/	/	
XOM	0	x	x	/	
XPO	0	x	x	/	

10.4.7 Chip verifiability

The table below lists ePassport issuing third countries and their verifiability. Complete readability (*i.e.* * at least SOD, DG1 and DG2 reading) is required.

In 97 % ePassports of countries with their CSCA certificate on the German Master List, are successfully verifiable. If the certificate is not available on the ML the electronic check quota is 100% undetermined.

Undetermined electronic checks results in most cases from missing certificates, expired certificates or irregularity of the "shell model".

Failed electronic checks mostly result from the Chip Authentication Check.

***Table 33** List of ePassport issuing third countries and their verifiability*

Country Code 3-letter	category # LOGs	electronic check successful [%]	electronic check failed [%]	electronic check undetermined [%]	CSCA available? (DE ML)
all TCN		85,76	0,04	14,20	
TCN on ML		96,63	0,01	3,36	
TCN not on ML		0,00	0,23	99,77	
ALB	II	0	0	100	0
AND	I	0	0	100	0
ARE	III	99,7	0	0,3	1
ARG	II	99,7	0,05	0,25	1
ARM	II	0	0	100	0
AUS	III	99,88	0	0,12	1
AZE	II	99,94	0	0,06	1
BDI	I	0	0	100	0
BEN	I	0	0	100	0
BHS	II	0	0	100	0
BIH	II	0	0	100	0
BRA	III	0	0,01	99,99	0
BRN	II	0	0	100	0
BWA	II	0	0	100	0
CAF	I	0	100	0	0
CAN	III	99,89	0	0,11	1
CHL	II	99,66	0	0,34	1
CHN	III	99,81	0,01	0,18	1
CIV	II	0	0	100	0
COG	I	0	100	0	0
COM	I	0	0	100	0

DZA	II	0	0,13	99,87	0
GAB	I	0	0	100	0
GEO	II	0	0,09	99,91	0
GIN	I	0	0	100	0
GMB	I	0	0	100	0
GNB	I	0	0	100	0
IDN	II	0	0	100	0
IND	I	0	0	100	0
IRN	III	0	1,74	98,26	0
ISR	II	99,98	0	0,02	1
JPN	III	99,81	0	0,19	1
KAZ	III	86,07	0	13,93	1
KHM	II	0	0,44	99,56	0
KNA	II	0	0	100	0
KOR	III	99,94	0	0,06	1
LSO	I	0	0	100	0
MAR	III	0	0	100	0
MCO	II	87,16	0	12,84	1
MDA	II	74,94	0	25,06	1
MDG	I	0	13,73	86,27	0
MDV	II	0	0	100	0
MKD	II	52,26	0	47,74	1
MNE	II	0	0	100	0
MNG	II	0	0	100	0
MOZ	II	0	0	100	0
MRT	II	0	0,58	99,42	0
MYS	III	59,45	0,38	40,17	1
NER	I	0	0	100	0
NGA	III	0	0,04	99,96	0
NZL	II	99,85	0	0,15	1
OMN	II	0	0	100	0
PAN	II	0	0	100	0
PHL	III	0	0	100	0
QAT	II	46,04	0	53,96	1
RKS	II	0	0	100	0
RUS	III	99,88	0	0,12	1
SDN	II	0	0	100	0
SEN	II	0	0	100	0
SGP	III	99,76	0	0,24	1
SMR	I	0	15,94	84,06	0
SOM	I	0	87,1	12,9	0
SRB	III	85,65	0	14,35	1
SSD	I	0	0	100	0
TGO	II	14,53	0	85,47	1
THA	III	37,51	0	62,49	1
TJK	II	32,98	0	67,02	1

TKM	II	0	0	100	0
TUR	III	99,59	0,02	0,39	1
TWN	III	98,76	0,16	1,08	1
UKR	II	0	1,04	98,96	0
UNO	II	0	0	100	1
USA	III	99,55	0	0,45	1
UZB	II	0	0	100	0
VAT	I	100	0	0	1
VCT	I	0	0	100	0
VEN	II	0	0	100	1
XOM	I	0	0	100	0
XPO	I	0	0	100	0

	count LOGs
Category I	< 100
Category II	between 100 and 10.000
Category III	> 10.000

Electronic check duration

The full electronic check process time is on average 3.9 seconds for third country ePassports. As it can be seen in the table below, the Nigerian ePassports are the fastest with 1.7 seconds due to BAC is not performed.

Table 34 *Electronic check process time*

Country Code 3-letter	category # LOGs	CSCA available? (DE ML)	AVG Electronic Checks Process time	AVG Chip Reading Duration	AVG Electronic Check Duration
all TCN			3,91	3,51	0,29
ALB	II	0	5,31	4,91	0,33
AND	I	0	3,93	3,38	0,3
ARE	III	1	5,24	4,54	0,62
ARG	II	1	3,38	2,76	0,27
ARM	II	0	6,92	6,34	0,4
AUS	III	1	5,12	4,75	0,29
AZE	II	1	4,3	3,82	0,38
BDI	I	0	3,79	3,32	0,22
BEN	I	0	2,5	2,06	0,26
BHS	II	0	5	4,58	0,34
BIH	II	0	5,42	4,88	0,46
BRA	III	0	2,82	2,31	0,35
BRN	II	0	3,56	2,96	0,33
BWA	II	0	3,96	3,51	0,28
CAF	I	0	3,37	2,37	0,68
CAN	III	1	3,31	2,79	0,27
CHL	II	1	7,35	6,67	0,47
CHN	III	1	3,85	3,43	0,25
CIV	II	0	1,91	1,54	0,26
COG	I	0	4	3,11	0,5
COM	I	0	2,73	2,39	0,23
DZA	II	0	3,07	2,71	0,28
GAB	I	0	3,97	3,87	0,08
GEO	II	0	5,21	4,73	0,41
GIN	I	0	4,69	4,26	0,26
GMB	I	0	3,2	2,9	0,25
GNB	I	0	3	2,49	0,2
IDN	II	0	4,7	4,25	0,28
IND	I	0	2,11	1,92	0,19
IRN	III	0	3,47	3,16	0,25
ISR	II	1	3,77	2,94	0,45
JPN	III	1	3,84	3,53	0,22
KAZ	III	1	3,9	3,42	0,27

KHM	II	0	2,2	1,79	0,3
KNA	II	0	5,07	4,63	0,38
KOR	III	1	2,78	2,43	0,27
LSO	I	0	2,39	1,91	0,43
MAR	III	0	2,77	2,39	0,28
MCO	II	1	2,73	2,49	0,22
MDA	II	1	3,06	2,46	0,33
MDG	I	0	3,45	3,08	0,22
MDV	II	0	4,49	3,92	0,39
MKD	II	1	4,2	3,79	0,35
MNE	II	0	3,42	2,94	0,25
MNG	II	0	3,18	2,39	0,74
MOZ	II	0	2,56	2,23	0,21
MRT	II	0	3,65	3,16	0,31
MYS	III	1	3,56	3,08	0,28
NER	I	0	3,48	2,87	0,3
NGA	III	0	1,66	1,23	0,32
NZL	II	1	4,14	3,79	0,28
OMN	II	0	2,02	1,52	0,37
PAN	II	0	7,16	6,73	0,24
PHL	III	0	2,97	2,42	0,26
QAT	II	1	4,21	3,73	0,27
RKS	II	0	3,77	3,39	0,3
RUS	III	1	5,39	4,99	0,32
SDN	II	0	3,96	3,33	0,29
SEN	II	0	3,06	2,66	0,29
SGP	III	1	2,35	1,95	0,28
SMR	I	0	4,52	4,17	0,17
SOM	I	0	2,31	2,12	0,16
SRB	III	1	3,21	2,81	0,34
SSD	I	0	3,36	2,9	0,22
TGO	II	1	4,07	3,78	0,22
THA	III	1	5,24	4,28	0,23
TJK	II	1	5,07	4,51	0,48
TKM	II	0	2,96	2,56	0,27
TUR	III	1	3,33	2,95	0,3
TWN	III	1	3,5	3,2	0,23
UKR	II	0	3,21	2,56	0,36
UNO	II	1	3,62	3,33	0,24
USA	III	1	4,52	4,15	0,28
UZB	II	0	3,88	3,4	0,38
VAT	I	1	4,63	4,19	0,27
VCT	I	0	3,17	2,65	0,18
VEN	II	1	4,38	4,07	0,23
XOM	I	0	3,33	2,75	0,26
XPO	I	0	9	5,27	3,15

	count LOGs
Category I	< 100
Category II	between 100 and 10.000
Category III	> 10.000

Legend:

Reading Duration = Time to read all files from chip (EF.COM, EF.SOD, DG1, DG2, conditionally DG14, DG15)

Check Duration = Time to perform Passive Authentication (including background system query)

Check Process time = Complete checking process (starting from optical reading trigger to end of check)

10.5Appendix 5: Iris spoofing

10.5.1 References

1. [Anjos2011] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," in International Joint Conference on Biometrics 2011, Oct. 2011
2. [Barsky2012] Barsky, T., Tankus, A. and Yeshurun, Y. Classification of fingerprint images to real vs. spoof. Int J. Biometrics 4(1) 2012.
3. [CESG01] Biometric Product Testing Final Report Issue 1.0 19 March 2001 - Tony Mansfield, Gavin Kelly, David Chandler, Jan Kane
4. [Chingovska2014] Biometrics Evaluation under Spoofing Attacks Ivana Chingovska, Andre Anjos, Sebastien Marcel. IEEE Transactions on Information Forensics and Security, 9(12):2264-2276, 2014. Available at: http://publications.idiap.ch/index.php/authors/show/921
5. [Cole] - Suspect Identities - A History of Fingerprinting and Criminal Identification, by Simon A. Cole, ISBN 9780674010024, October 2002
6. [FASTPASS] - Biometrics in ABC: counter-spoofing research, Hong Wei, Lulu Chen, James M Ferryman, Computational Vision Group, downloadable from https://www.fastpass-project.eu/sites/default/files/paper-biometrics%20ABC-final%20version.pdf
7. [Galbally1] – Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms, by Javier Galbally et al, published in Computer Vision and Image Understanding, Volume 117, Issue 10, October 2013
8. [Galbally2] – Securing Iris Recognition Systems Against Masquerade Attacks, by Javier Galbally et al, Published in SPIE Proceedings Vol. 8712: Biometric and Surveillance Technology for Human and Activity Identification X, Ioannis Kakadiaris et al, June 2013
9. [Li2004] J. Li, Y. Wang, T. Tan, and A. Jain, "Live face detection based on the analysis of fourier spectra," Biometric Technology for Human Identification, vol. 5404, pp. 296–303, 2004
10. [Pan2012] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based antispoofing in face recognition from a generic webcamera," in Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on Computer Vision, pp. 1–8, IEEE, 2007.
11. [Pereira2013] José Mario de Martino, Sebastien Marcel, André Anjos Rabello and Tiago de Freitas Pereira, Can face anti-spoofing countermeasures work in a real world scenario?, in: International Conference on Biometrics, Madrid, Spain, 2013
12. [Ruiz2008] - Direct Attacks Using Fake Images in Iris Verification, by Virginia Ruiz-Albacete et al, published in LNCS, B. Schouten et al. (Eds.): BIOID 2008, LNCS 5372, pp. 181–190, 2008.
13. An overview of face liveness detection, Saptarshi Chakraborty and Dhrubajyoti Das, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014
14. [SEC2DFACE] Second Competition on Counter Measures to 2D Face Spoofing Attacks, I. Chingovska, J. Yang, Z. Lei, D. Yi, S. Z. Li, O. K¨ahm, C. Glaser, N. Damer, A. Kuijper, A. Nouak,, J. Komulainen, T.

Pereira, S. Gupta, S. Khandelwal, S. Bansal, A. Rai, T. Krishna, D. Goyal, M.-A. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, M. Gabbouj, R. Tronci, M. Pili, N. Sirena, F. Roli, J. Galbally, J. Fierrez, A. Pinto, H. Pedrini, W. S. Schwartz, A. Rocha, A. Anjos, S. Marcel

15. Tabula Rasa reference list: https://www.tabularasa-euproject.org/publications/index.php
16. [Trefny2010] J. Trefn ` y and J. Matas, "Extended set of local binary patterns for rapid object detection," in Proceedings of the Computer Vision Winter Workshop, vol. 2010, 2010

10.5.2 References to biometric Protection Profiles

Archived: U.S. Government Approved Protection Profile - U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 1.0, http://www.niap-ccevs.org/pp/PP_BVM_BR_V1.0/, Date: 12 January 2006 – Common Criteria Version: 2.3 - Not assigned to any Validated Products

Archived: U.S. Government Approved Protection Profile - U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.1, http://www.niap-ccevs.org/pp/PP_BVM_MR_V1.1/ Date: 25 July 2007 – Common Criteria Version: 2.3, - Not assigned to any Validated Products

Biometric Device Protection Profile (BDPP), http://www.cesg.gov.uk/policy_technologies/biometrics/media/bdpp082.pdf, **Date:** 5. September 2001 – Common Criteria Version: 2.3, (unclear whether this was ever used)

Protection Profile - Biometric Verification Mechanisms Version 1.04, (BSI-PP-0016-2005) – Evaluated PP, https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0016, **Date:** 17. August 2005 – Common Criteria Version: 2.3, Based on PP 1. - 3. – Used for 2 Products – 1 under re-evaluation

Biometric Verification Mechanisms Protection Profile Version 1.3, (BSI-CC-PP-0043-2008) – Evaluated PP, https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0016, **Date:** 07. August 2008 – Common Criteria Version: 3.1 Rev 2

Fingerprint Spoof Detection Protection Profile (FSDPP), Version 1.8, (BSI-CC-PP-0063-2010), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0063b_pdf.pdf?__blob=publicationFile, Date: 23th November, 2009 – Common Criteria Version: 3.1 Rev 3, 2 Products under evaluation (2014)

Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, (BSI-CC-PP-0062-2010), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0062b_pdf.pdf?__blob=publicationFile, Date: 27th November 2009 – Common Criteria Version: 3.1 Rev 3

10.5.3 References relevant to iris spoofing

====legacy====

Iris liveliness:

[Ruiz2008] - Direct Attacks Using Fake Images in Iris Verification, by Virginia Ruiz-Albacete et al, published in

LNCS, B. Schouten et al. (Eds.): BIOID 2008, LNCS 5372, pp. 181–190, 2008.

J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," 2012,

G. Erdogan and A. Ross, "Automatic Detection of Non-cosmetic Soft Contact Lenses in Ocular Images," Proc. of SPIE Biometric and Surveillance Technology for Human and Activity Identification X, (Baltimore, USA), May 2013.
http://www2.cse.msu.edu/~rossarun/pubs/GizemRossContactLens_SPIE2013.pdf

[This paper detects non-cosmetic *soft* contact lenses]

J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, J. Ortega-Garcia,
"Iris Image Reconstruction from Binary Templates: An Efficient Probabilistic Approach Based on Genetic Algorithms,"
Computer Vision and Image Understanding, Vol. 117, Issue 10, pp. 1512 - 1525, October 2013.
http://www2.cse.msu.edu/~rossarun/pubs/GalballyRossIrisReconstruction_CVIU2013.pdf
[This paper shows that iris images can be reverse engineered from their iris codes].

J. Galbally, M. Gomez-Barrero, A. Ross, J. Fierrez, J. Ortega-Garcia,
"Securing Iris Recognition Systems Against Masquerade Attacks,"
Proc. of SPIE Biometric and Surveillance Technology for Human and Activity Identification X, (Baltimore, USA), May 2013.
https://www.beat-eu.org/publications/index.php/attachments/single/31
[This paper presents methods to mitigate masquerade attacks in iris recognition]

Unraveling the Effect of Textured Contact Lenses on Iris Recognition,

Daksha Yadav, Naman Kohli, James S. Doyle, Rich Singh, Mayank Vatsa and

Kevin W. Bowyer, IEEE Transactions on Information Forensics and Security 9 (5), 851-862, May 2014.

http://www3.nd.edu/~kwb/YadavEtAlTIFS_2014.pdf

Variation in Accuracy of Textured Contact Lens Detection Based on Iris Sensor and Contact Lens Manufacturer, James S. Doyle, Kevin W. Bowyer and Patrick J. Flynn,

Biometrics Theory, Applications and Systems (BTAS), Sept 30 - Oct 2, 2013.

http://www3.nd.edu/~kwb/DoyleBowyerFlynnBTAS_2013.pdf

Detection of Contact-Lens-Based Iris Biometric Spoofs Using Stereo Imaging,

Ken Hughes and Kevin W. Bowyer,

Hawaii International Conference on System Sciences (HICSS 46), January 7-10, 2013. http://www3.nd.edu/~kwb/HughesBowyerHICSS_2013.pdf

Pupil Dynamics for Iris Liveness Detection

Adam Czajka,

IEEE Transactions on Information Forensics and Security, April 2015.

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7029052

10.5.4 References relevant to spoofing

NIST, ISO, BSI, last LivDet reports, as well as publications from

- **Tabula Rasa project**

The material is downloadable from https://www.tabularasa-euproject.org/

- **Fidelity**

The material from this project with regard to the ePassport life cycle management is available at http://www.fidelity-project.eu

- **UIDAI**
- **ICAO**

[ICAO9303P1V2] ICAO Doc 9303 Part 1 Machine readable passports Volume 2 Specifications for electronically enabled passports with biometric identification capability (2006)

[ICAO9303P3V2] ICAO Doc 9303 Part 3 MRTD Volume 2 MRD with biometrics (2008)

[ICAO9303SUP] Supplement to Doc 9303 Version: Release 14 Status: Final (2014)

- **Spoofing and presentation attacks**

Biometrics in ABC: counter-spoofing research, Hong Wei, Lulu Chen, James M Ferryman, Computational Vision Group, downloadable from https://www.fastpass-project.eu/sites/default/files/paper-biometrics%20ABC-final%20version.pdf

An overview of face liveness detection, Saptarshi Chakraborty and Dhrubajyoti Das, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014

Pubic Final Report "Evaluation of fingerprint recognition technologies – BioFinger", Bundesamt for Sicherheit in der Informationstechnik, Bundeskriminalamt, Fraunhofer (2004)

- **Tabula Rasa publications list**

https://www.tabularasa-euproject.org/publications/index.php

- **Other topics:**

N. Kose and J. .-L. Dugelay, "Classification of Captured and Recaptured Images to Detect Photograph Spoofing," 2012,
X. Zhao, N. Evans, and J. .-L. Dugelay, "Semi-supervised Face Recognition with LDA Self-training," 2011,
A. Anjos and S. Marcel, "Counter-Measures to Photo Attacks in Face Recognition: a public database and a baseline," 2011,

Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "A method for performance evaluation of multi-modal biometric systems under spoofing attacks," 2011,

J. Ylioinas, A. Hadid, and M. Pietikäinen, "Combining contrast information and local binary patterns for gender classification," 2011,

A. Hadid, J. .-L. Dugelay, and M. Pietikäinen, "On the Use of Dynamic Features in Face Biometrics: Recent Advances and Challenges," Journal on Signal Image and Video Processing, 2011.

M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Z. Li, W. R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrillón-Santana, J. Määttä, A. Hadid, and M. Pietikäinen, "Competition on Counter Measures to 2-D Facial Spoo fing Attacks," 2011,

Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Performance Prediction of Biometric Systems under Spoof Attacks," 2011,

J. Määttä, A. Hadid, and M. Pietikäinen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis," 2011,

G. Zhao, X. Huang, M. Taini, S. Z. Li, and M. Pietikäinen, "Facial expression recognition from near-infrared videos," Image and Vision Computing, 2012.

X. Zhao, N. Evans, and J. .-L. Dugelay, "A Co-training Approach to Automatic Face Recognition," 2011,

M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Hill-Climbing Attack Based on the Uphill Simplex Algorithm and its Application to Signature Verification," 2011,

J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A High Performance Fingerprint Liveness Detection Method Based on Quality Related Features," Future Generation Computer Systems, 2012.

A. Hadid, "Analyzing facial behavioural features from video," 2011,

A. Hadid and M. Pietikäinen, "Demographic Classification From Face Videos Using Manifold Learning," Neurocomputing, 2012.

R. Wallace, M. McLaren, C. McCool, and S. Marcel, "Inter-session Variability Modelling and Joint Factor Analysis for Face Authentication," 2011,

Z. Akthar, B. Biggio, G. Fumera, and G. L. Marcialis, "Robustness of Multimodal Biometric Systems under Realistic Spoof Attacks against All Traits," 2011,

J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of Direct Attacks to Fingerprint Verification Systems," Telecommunication Systems, 2011.

M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "An evaluation of indirect attacks and countermeasures in fingerprint verification systems," Pattern Recognition Letters, 2011.

Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Robustness Evaluation of Biometric Systems under Spoof Attacks," 2011,

Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Robustness analysis of likelihood ratio score fusion rule for multimodal biometric systems under spoof attacks," 2011,

E. Mordini and A. P. Rebera, "No Identification without Representation: Global Policy Issues Raised By Large-Scale Biometric Identification," Review of Policy Research, 2012.

R. Wallace, M. McLaren, C. McCool, and S. Marcel, "Cross-pollination of normalisation techniques from speaker to face authentication using Gaussian mixture models," IEEE Transactions on Information Forensics and Security, 2012.

Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of multi-modal biometric score fusion rules under spoof attacks," 2012,

D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "Fingerprint Liveness Detection Competition 2011," 2012,

Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A Face Antispoofing Database with Diverse Attacks," 2012,

Z. Lei, C. Zhou, D. Yi, A. K. Jain, and S. Z. Li, "An Improved Coupled Spectral Regression for Heterogeneous Face Recognition," 2012,

F. Alegre, R. Vipperla, and N. Evans, "Spoofing countermeasures for the protection of automatic speaker recognition from attacks with artificial signals," in Proc. Proceedings of INTERSPEECH 2012, 2012,

J. Zhu, D. Cao, S. Liu, Z. Lei, and S. Z. Li, "Discriminant Analysis with Gabor Phase for Robust Face Recognition," 2012,

M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Face verification put to test: a hill-climbing attack based on the uphill-simplex algorithm," 2012,

B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Robustness of multimodal biometric verification systems under realistic spoofing attacks," 2011,

Z. Lei, D. Yi, and S. Z. Li, "Discriminant Image Filter Learning for Face Recognition with Local Binary Pattern Like Representation," in Proc. Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition, 2012,

G. L. Marcialis, P. Coli, and F. Roli, "Fingerprint Liveness Detection based on Fake Finger characteristics," International Journal of Digital Crime and Forensics, 2012.

L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint Liveness Detection by Local Phase Quantization," in Proc. Proceedings of 21st Int. Conf. On Pattern Recognition, 2012,

Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc. Proceedings of 5th International Conference on Biometrics: Theory, Applications, and Systems, 2012,

B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," IET Biometrics, 2012.

N. Erdogmus, N. Kose, and J. .-L. Dugelay, "Impact Analysis of Nose Alteration on Face Recognition Performances," in Proc. Proceedings of MMSP 2012, 2012,

N. Kose, N. Erdogmus, and J. .-L. Dugelay, "Block Based Face Recognition Approach Robust to Nose Alteration," in Proc. Proceedings of BTAS 2012, 2012,

L. Ghiani, G. L. Marcialis, and F. Roli, "Experimental Results on the Feature-level Fusion of Multiple Fingerprint Liveness Detection Algorithms," in Proc. Proceedings of 14th ACM Workshop on Multimedia and Security, 2012,

L. Ghiani, P. Denti, and G. L. Marcialis, "Experimental Results on Fingerprint Live- ness Detection," in Proc. Proceedings of 7th Int. Conference on Articulated Motion and Deformable Objects, 2012,

D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011 - Fingerprint Liveness Detection Competition 2011," 2012,

J. Ylioinas, A. Hadid, and M. Pietikäinen, "Age Classification in Unconstrained Conditions Using LBP Variants," in Proc. Proceedings of ICPR 2012, 2012,

S. Liu, D. Yi, Z. Lei, and S. Z. Li, "Heterogeneous Face Image Matching Using Multiscale Features," 2012,

A. Hadid, V. Ghahramani, V. Kellokumpu, M. Pietikäinen, J. Bustard, and M. Nixon, "Can Gait Biometrics be Spoofed?" in Proc. Proceedings of ICPR 2012, 2012,

E. Mordini and A. P. Rebera, "Conceptualizing the Biometric Body," Yearbook 2012 of Digital Enlightenment Forum, 2012.

Z. Lei, Z. Zhang, and S. Z. Li, "Feature Space Locality Constraint for Kernel based Non- linear Discriminant Analysis," Pattern Recognition, 2012.

Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Regularized Transfer Boosting for Face Detection Across Spectrum," IEEE Signal Processing Letters, 2012.

Z. Lei, S. Liao, and S. Z. Li, "Efficient Feature Selection for Linear Discriminant Analysis and Its Application to Face Recognition," in Proc. Proceedings of International Conference on Pattern Recognition, 2012,

I. Chingovska, A. Anjos, and S. Marcel, "On the Effectiveness of Local Binary Patterns in Face Anti-spoofing," in Proc. Proceedings of BioSIG 2012, 2012,

A. Anjos, L. El-Shafey, R. Wallace, M. Guenther, C. McCool, and S. Marcel, "Bob: a free signal processing and machine learning toolbox for researchers," in Proc. Proceedings of ACM MM 2012, 2012,

F. Alegre, R. Vipperla, N. Evans, and B. Fauve, "On the vulnerability of automatic speaker recognition to spoofing attacks with artificial signals," in Proc. EUSIPCO 2012, 2012,

T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in Proc. International Conference on Biometrics, 2013,

T. Huynh, R. Min, and J. .-L. Dugelay, "An efficient LBP-based descriptor for facial depth images applied to gender recognition using RGB-D face data," in Proc. Proceedings of the Workshop on Computer Vision with Local Binary Pattern Variants, 2012,

F. Alegre, A. Fillatre, and N. Evans, "Spoofing countermeasures to protect automatic speaker verification from voice conversion," in Proc. Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, 2013,

J. Komulainen, A. Hadid, M. Pietikäinen, A. Anjos, and S. Marcel, "Complementary Countermeasures for Detecting Scenic Face Spoofing Attacks," in Proc. International Conference on Biometrics, 2013,

J. Ylioinas, A. Hadid, Y. Guo, and M. Pietikäinen, "Efficient image appearance description using dense sampling based local binary patterns," in Proc. Proceedings of the Asian Conference on Computer Vision, 2012,

J. Bustard, J. N. Carter, and M. Nixon, "Targeted biometric impersonation," in Proc. Proceedings of the

Workshop on Biometrics and Forensics, 2013,

B. Biggio, G. Fumera, and F. Roli, "Security evaluation of pattern classifiers under attack," IEEE Trans. on Knowl. and Data Engineering, 2013.

B. Biggio, L. Didaci, G. Fumera, and F. Roli, "Poisoning attacks to compromise face templates," in Proc. International Conference on Biometrics, 2013,

N. Kose and J. .-L. Dugelay, "Countermeasure for the Protection of Face Recognition Systems Against Mask Attacks." in Proc. Proceedings of the 10th IEEE International Conference on Automatic Face and Gesture Recognition, 2013,

X. Feng, Y. Lai, X. Peng, X. Jiang, and A. Hadid, "Extracting Local Binary Patterns from image key points: application to automatic facial expression recognition," in Proc. Proc. 18th Scandinavian Conference on Image Analysis (SCIA2013), 2013,

J. Komulainen, A. Hadid, and M. Pietikäinen, "Face spoofing detection using dynamic texture," in Proc. Proceedings of ACCV Workshop on Computer Vision with Local Binary Pattern Variants (LBP 2012), 2012,

N. Kose and J. .-L. Dugelay, "Shape and Texture Based Countermeasure to Protect Face Recognition Systems Against Mask Attacks." in Proc. IEEE Computer Society Workshop on Biometrics (CVPRW 2013), 2013,

N. Kose and J. .-L. Dugelay, "Reflectance Analysis Based Countermeasure Technique to Detect Face Mask Attacks," in Proc. IEEE International Conference on Digital Signal Processing (DSP 2013), 2013,

Y. Jianwei, L. Zhen, L. Shengcai, and S. Z. Li, "Face Liveness Detection with Component Dependent Descriptor," in Proc. In Proceedings of the 6th IAPR International Conference on Biometrics, (ICB2013), 2013,

T. Wang, Y. Jianwei, L. Zhen, L. Shengcai, and S. Z. Li, "Face Liveness Detection Using 3D Structure Recovered from a Single Camera," in Proc. In Proceedings of the 6th IAPR International Conference on Biometrics, (ICB2013), 2013,

J. Yan, X. Zhang, L. Zhen, D. Yi, and S. Z. Li, "Structural Models for Face Detection," in Proc. In Proceedings of the 10th IEEE International Conference on Automatic Face and Gesture Recognition, (FG2013), 2013,

J. Yan, X. Zhang, L. Zhen, D. Yi, and S. Z. Li, "Real-time High Performance Deformable Model for Face Detection in the Wild," in Proc. n Proceedings of the 6th IAPR International Conference on Biometrics, (ICB2013), 2013,

Z. Cai, L. Wen, D. Cao, Z. Lei, D. Yi, and S. Z. Li, "Person-Specific Face Tracking with Online Recognition," in Proc. In Proceedings of the 10th IEEE International Conference on Automatic Face and Gesture Recognition, (FG2013), 2013,

N. Kose and J. .-L. Dugelay, "On the Vulnerability of Face Recognition Systems to Spoofing Mask Attacks," in Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2013), 2013,

A. P. Rebera, M. E. Bonfanti, and S. Vernier, "Societal and Ethical Implications of Anti-Spoofing Technologies in Biometrics," Science and Engineering Ethics, 2013.

E. Mordini, "The Two Horns of Forensic Biometrics," EUROPEAN ASSOCIATION FOR BIOMETRICS (EAB) NEWSLETTER, 2013.

Spoofing and countermeasures for automatic speaker verification, 2013.

N. Evans, J. Yamagishi, and T. Kinnunen, "Spoofing and counter- measures for speaker verification: a need for standard corpora, protocols and metrics," IEEE Signal Processing Society Newsletter, 2013.

F. Alegre, R. Vipperla, A. Amehraye, and N. Evans, "A new speaker verification spoofing countermeasure based on local binary patterns," in Proc. 14th Annual Conference of the International Speech Communication Association. 2013,

F. Alegre, R. Vipperla, A. Amehraye, and N. Evans, "A one- class classification approach to generalised speaker verification spoofing countermea- sures using local binary patterns," in Proc. Proceedings of the International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013,

J. Bustard, J. N. Carter, and M. Nixon, "Targeted Impersonation As A Tool For The Detection Of Biometric System Vulnerabilities," in Proc. Proceedings of the International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013,

L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, "Ingerprint Liveness Detection us- ing Bizanized Statistical Image Features," in Proc. IEEE 6th International Conference on Biometrics: Theory, Applications, and Systems, (BTAS 2013), 2013,

10.6 Appendix 6: VIS

Even if the verification of fingerprints has not been explicitly covered in the previous points, from a legal perspective this is a mandatory step of the border check for visa holders. In order to enable this possibility, the following approach is suggested:

- The new search operation that would be used at first line to consult VIS with TDN will also allow the verification of the attached fingerprints;
- The operation will be executed to obtain the relevant application record;
- VIS will automatically extract from that application record the identifier which will allow it to execute the verification of fingerprints of VIS. This execution would be very similar to the current AuthenticateByFingerprint operation and will be performed in a transparent way;
- A response, specifying whether the verification has been successful or not, will be sent back to the border guard.

Cases where a list of visa records with a valid visa for a given TDN is returned, will be treated as exceptions. In these regard, the following approach could be envisaged:

- The border guard will have to manually select from the list the relevant record and retrieve its information. In order to verify the fingerprints the operation AuthenticateByFingerprint will have to be executed by sending to VIS both the VSN and the fingerprints to be verified;
- Another option could be that the fingerprints that have been sent to VIS are used to discriminate which is the relevant record from the list. To achieve this, the central system would have to try to match the fingerprints with the ones stored for those records; the record for which the verification results in a hot will be returned to the border guard.
  - This option has its own limitations, as there are cases where the fingerprints might not be present in VIS.

10.7Appendix 7: Bibliography

- **FRONTEX. 2011.** Best Practice Guidelines on the Design, Deployment and Operation of Automated BorderCrossing Systems Crossing Systems . 2011.

  —. 2012. Best Practice Operational Guidelines for Automated Border Control (ABC) Systems. 2012.